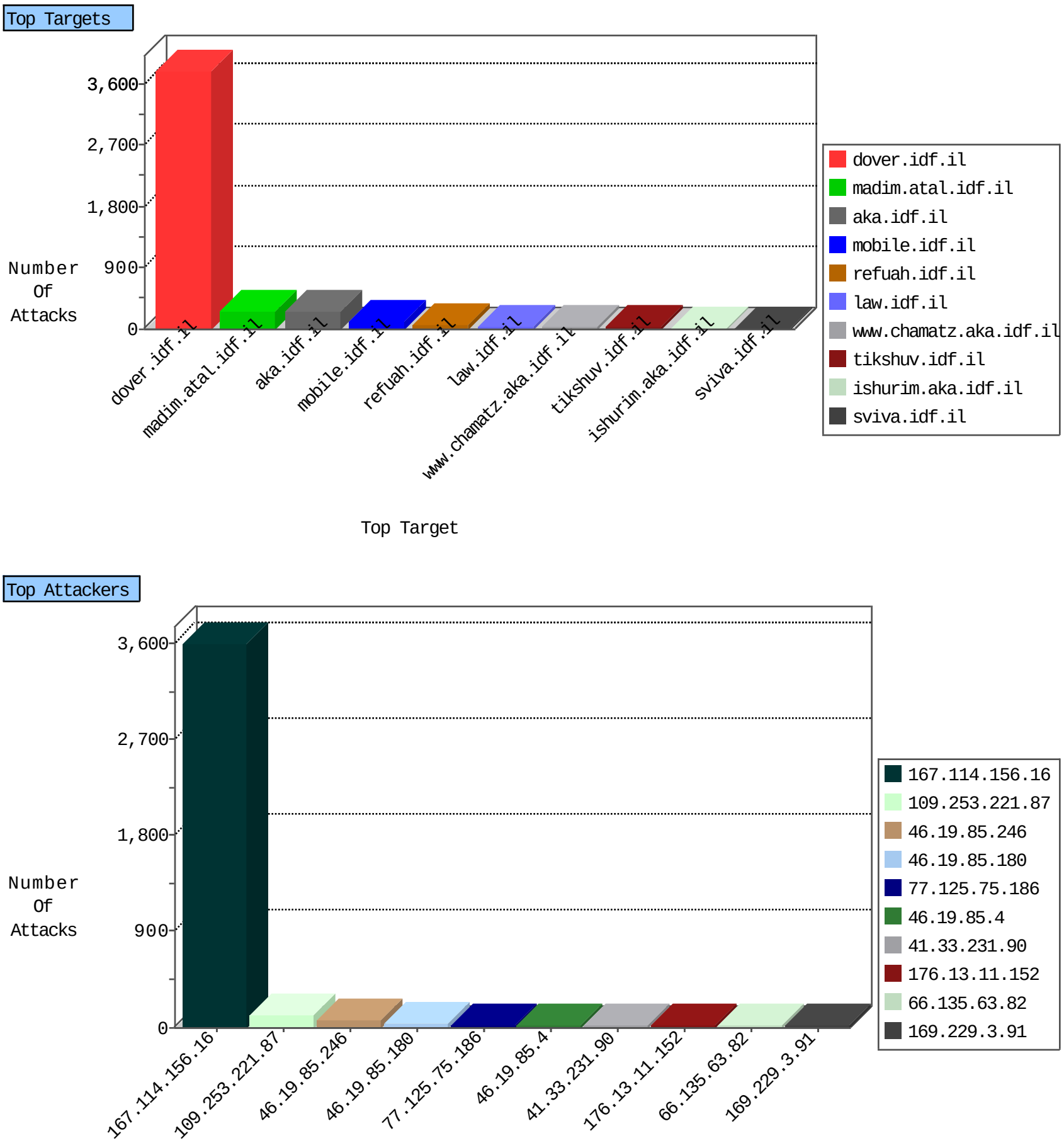
04-14-2016-14:04:06 to 04-14-2016-15:04:06

IDF Under Attack
Daily Report



04-14-2016-14:04:06 to 04-14-2016-15:04:06

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	3603
82.145.209.190	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	4
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.46.102.242	Romania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1

04-14-2016-14:04:06 to 04-14-2016-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.144.214	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
213.8.145.99	Israel	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
41.185.31.40	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.135.63.82	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.135.63.82	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.106.179.116	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
209.173.241.141	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.176.124.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.48.104.140	Netherlands	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	1
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
151.80.31.176	France	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.161	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.181	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.163	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.169	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.175	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

04-14-2016-14:04:06 to 04-14-2016-15:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.135.63.82	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	13
209.173.241.141	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	9
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	8
87.106.179.116	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	7
41.185.31.40	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	7
95.211.70.193	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
85.64.229.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
82.81.55.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.97	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.56.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.222.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.24.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
85.64.72.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.15.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.5.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.194.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.130.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.53.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-14-2016-14:04:06 to 04-14-2016-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.13.11.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.130.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.100	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	12
93.172.155.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.53.191.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.139.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.16.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
193.47.165.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.35.16.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
5.102.195.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.114.23.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.31.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.16.15	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.79.123	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.123	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.124	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
109.65.144.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.177.104.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.177.104.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.94.106	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.176.124.194	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.195.133	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.34	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.34	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
95.86.98.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.22.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.20.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.130.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.179.215.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.147.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.23.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.217.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
132.71.80.25	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.13.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.136.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.117.105.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.217.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	12
2.53.130.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.15.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.130.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
93.172.253.145	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	4
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx'	Block	3
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	3
37.48.104.140	Netherlands	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
212.199.176.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
2.55.29.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	3
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.21.30	Block	3
2.55.41.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	2
64.62.219.79	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
37.48.104.140	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.48.104.140	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
2.53.191.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
93.172.253.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/9/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
184.14.139.16	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
46.117.101.174	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Abnormally Long Request	Block	1
77.125.75.186	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
37.48.104.140	Netherlands	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
66.249.79.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.25.79.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
2.53.189.27	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
120.132.50.135	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.qunar.com/894-he/atal.aspx	Block	1
82.166.140.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx/	Block	1
77.125.75.186	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding ¸|xxÚ%[[:#27ıı@]]t½3²'•:”	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.163.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx'	Block	1
109.253.128.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
184.14.139.16	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1