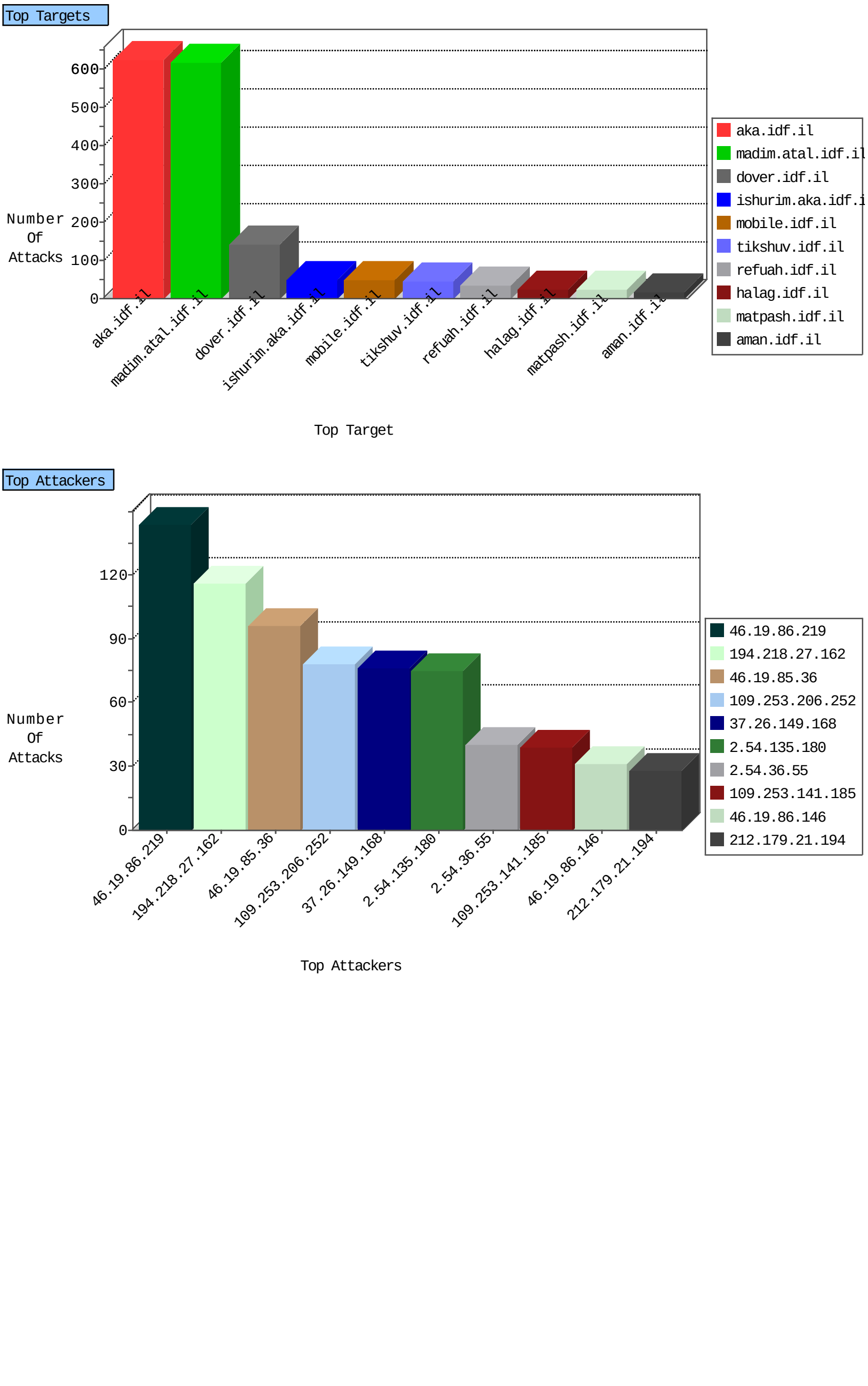
03-01-2016-13:04:01 to 03-01-2016-14:04:01

IDF Under Attack Daily Report



03-01-2016-13:04:01 to 03-01-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.211.18	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
31.168.133.226	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
212.71.235.23	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
173.234.39.194	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
52.53.222.9	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.251	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-13:04:01 to 03-01-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.214.46	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	15
81.218.135.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
188.120.151.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
37.26.146.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.183.191.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.167.17	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
37.26.147.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.152.18	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
80.179.15.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
136.243.152.18	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.170.165	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
80.246.133.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
162.210.196.98	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
87.117.15.10	Russian Federation	147.237.0.34	tikshuv.idf.il	C1000016: HTTP: administrator in URI	Block	1

03-01-2016-13:04:01 to 03-01-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.57.11.7	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
68.168.213.121	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -f -sS	1
192.117.171.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.60.42.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.66.152.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.61.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.142.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.25.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.112.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
68.168.213.121	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
61.244.49.137	147.237.76.147	Hong Kong	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.3.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.75.156.161	147.237.77.216	Czech Republic	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.196.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.228.248.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.36.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.36.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.152.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.84.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-01-2016-13:04:01 to 03-01-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	75
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	41
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.178.1.34	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
2.54.36.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.54.3.46	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.195.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.76.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.215.227.251	France	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	8
185.120.126.53		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.36.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.16.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.36.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
2.54.166.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.28.184.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.34.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.181.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.125.148.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.246.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.244.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.111.170.206	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.36.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.17.161	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.26.228	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.153.242	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	5
80.246.136.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.36.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.36.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.32.179.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.178.51.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.230.86.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.34.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.179.104	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.149.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	4
185.24.207.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.174.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.149.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
157.55.39.253	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.172.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.27.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.199.34.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
188.238.95.106	Finland	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
2.54.174.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	144
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
109.253.206.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
2.54.135.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
37.26.149.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
109.253.141.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.253.129.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
37.26.147.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.20.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
87.71.21.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.71.21.122	Block	7
5.29.103.206	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.103.206	Block	6
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.54.22.36	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	4
212.25.107.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	4
176.13.0.27	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	4
46.19.86.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.19.85.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.13.63	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
109.253.136.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.56.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/9/	Block	3
5.102.196.228	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.102.196.228	Block	3
80.246.136.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.145.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.25.107.145	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 212.25.107.145	Block	2
5.29.103.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.117.15.10	Russian Federation	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	2
5.102.196.228	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
80.246.136.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.154.235.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.60.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.7.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.76.98.80	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.98.80	Block	1
192.118.78.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rules.abe	Block	1
80.161.191.25	Denmark	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/robots.txt	Block	1
5.102.196.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/ajax/updatestatus.php	Block	1
64.62.219.148	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.117.15.10	Russian Federation	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
212.25.102.182	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
81.218.22.216	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.law.idf.il/421-he/patzar.aspx	Block	1
79.178.103.187	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
54.213.103.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1