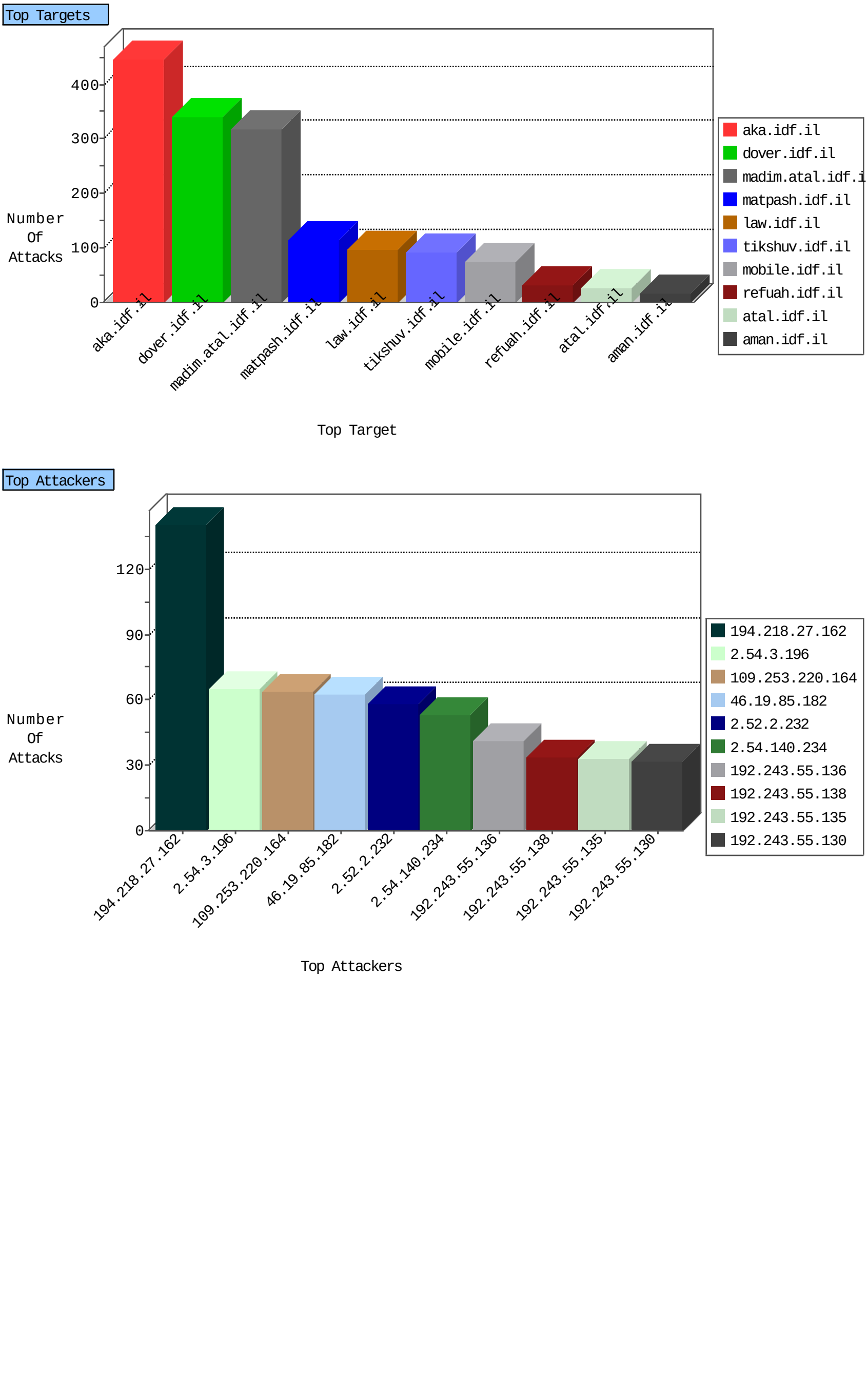
03-02-2016-10:04:04 to 03-02-2016-11:04:04

IDF Under Attack
Daily Report



03-02-2016-10:04:04 to 03-02-2016-11:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
80.179.102.94	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
80.246.136.3	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
84.108.233.193	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
8.37.237.35	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
8.37.237.35	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.99.63.194	Canada	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
192.99.63.194	Canada	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
188.138.102.50	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
119.42.83.119	Thailand	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
192.99.63.194	Canada	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
192.99.63.194	Canada	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
164.132.54.194	Italy	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.110	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
83.172.77.39	Sweden	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1

03-02-2016-10:04:04 to 03-02-2016-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
81.218.101.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
144.76.7.107	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
46.19.86.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.60.47.239	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
5.9.85.4	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.7.107	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.147.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.115.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.3	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.79	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
80.178.143.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
40.85.142.106	United States	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.57	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
80.246.130.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
40.85.142.106	United States	147.237.0.17	m.my-kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
51.255.65.61	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
80.246.133.64	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
40.85.142.106	United States	147.237.0.19	madim.atal.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
51.255.65.83	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-02-2016-10:04:04 to 03-02-2016-11:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.57.113.2	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.115.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
60.18.162.244	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 4096	1
213.151.47.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.34.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.36.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.52.158.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.66.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.232.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.48.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.112.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
60.18.162.244	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.202.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.76.176	Latvia	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.7.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.254.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.165.135.130	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

03-02-2016-10:04:04 to 03-02-2016-11:04:04

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	95
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	46
82.81.101.178	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
82.81.101.179	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
85.130.132.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.150.29.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.86.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.12.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	9
176.13.3.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.0.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.182.48.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.254.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.155.252.47	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.20.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.199.185.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.125.94.148	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.130.132.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.32	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.179.225.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.130.132.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.150.29.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.138.12.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
132.70.66.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.150.29.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.3.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
109.253.220.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
46.19.85.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
2.52.2.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.54.140.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	8
176.13.3.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	6
2.54.32.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
213.6.150.158	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	4
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 209.88.198.1	Block	4
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	4
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.7.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.163.189	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.29.163.189	Block	3
78.40.177.35	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
132.3.21.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.48.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
217.132.132.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.132.132.72	Block	3
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
147.235.8.76	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
132.3.21.78	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.45.62.147	Czech Republic	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
5.29.163.189	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
84.94.18.133	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.86.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/payslips.aspx	Block	2
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	2
217.132.132.72	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
132.3.21.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	2
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl53.y in www.aka.idf.il/main/sachar/payslips.aspx	None	2
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
217.132.132.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
37.26.148.140	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.45.62.147	Czech Republic	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 2	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method é/yÚ[[#22]]Ð†%_ò´Ó[[#14]]×	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
5.45.62.147	Czech Republic	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
138.134.102.15	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl04.y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
54.213.177.200	United States	147.237.76.39	mobile.meitav.idf.il	NULL Character in Method	Block	1
183.15.100.49	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/5/785.pdf/rk=0/rs=axzlwggpuqw0ysjnt5ua.p2ooqy-	Block	1
2.54.14.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1