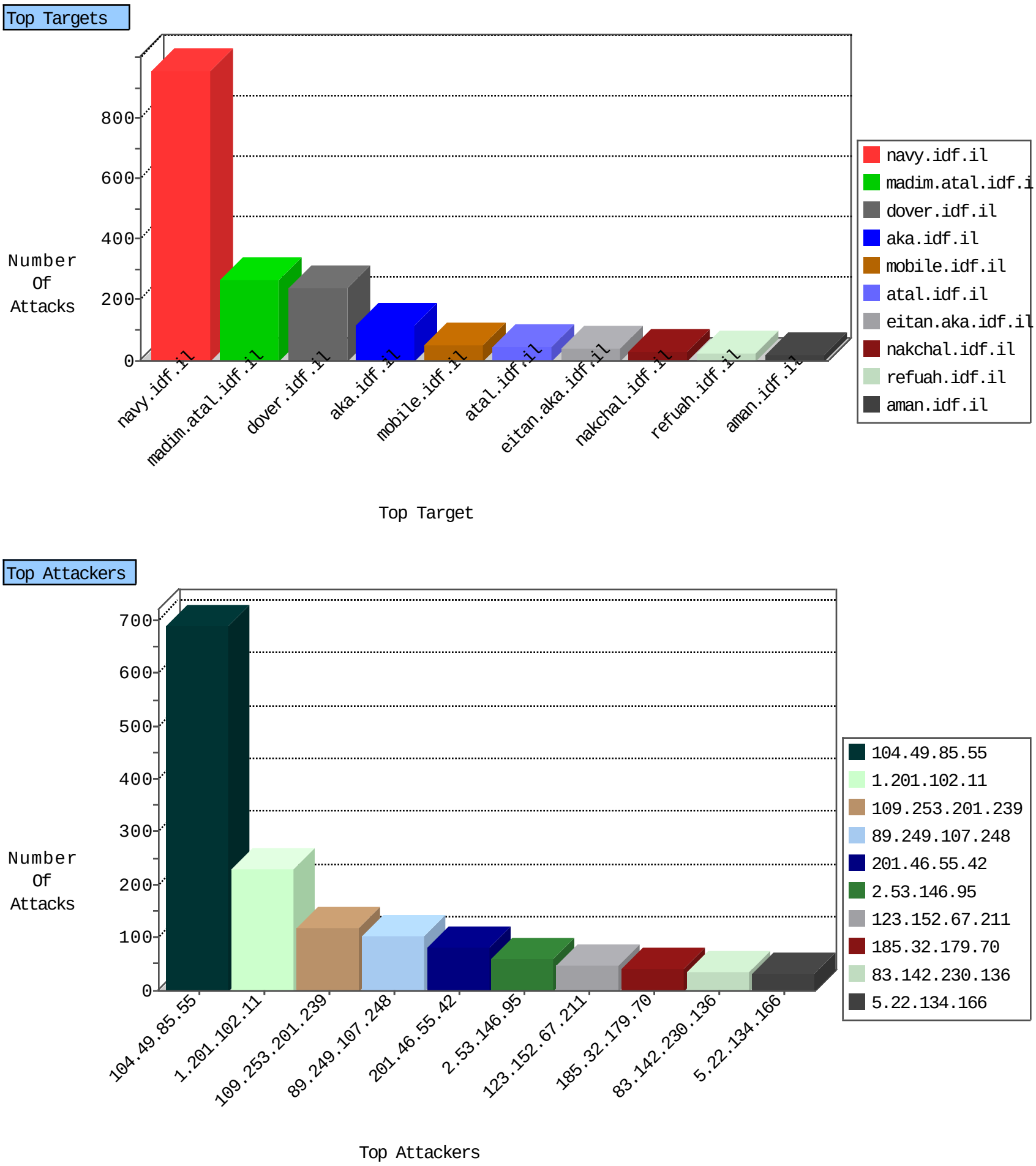
09-05-2016-10:09:33 to 09-05-2016-11:09:33

IDF Under Attack Daily Report



09-05-2016-10:09:33 to 09-05-2016-11:09:33

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.234.124	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
83.142.230.136	United Kingdom	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Http	drop	1
217.23.9.123	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1

09-05-2016-10:09:33 to 09-05-2016-11:09:33

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.205.218	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
83.142.230.136	United Kingdom	147.237.76.42	refuah.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
83.142.230.136	United Kingdom	147.237.76.86	navy.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
83.142.230.136	United Kingdom	147.237.76.30	himush.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
83.142.230.136	United Kingdom	147.237.76.147	chinuch.aka.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
83.142.230.136	United Kingdom	147.237.76.31	nakchal.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
83.142.230.136	United Kingdom	147.237.76.200	eitan.aka.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
83.142.230.136	United Kingdom	147.237.76.39	mobile.meitav.idf.il	16907: HTTP: FHScan Core Scanner Usage	Block	2
185.120.124.12	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
89.234.157.254	France	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-05-2016-10:09:33 to 09-05-2016-11:09:33

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.245.205.76	147.237.76.31	Russian Federation	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
195.245.205.76	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.72.217	Russian Federation	e.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.77.176	Russian Federation	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.76.42	Russian Federation	refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
82.80.192.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.212	Russian Federation	e.dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
193.106.206.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.67.104.51	147.237.76.42	Spain	refuah.idf.il	ET SCAN Potential SSH Scan	1
195.245.205.76	147.237.77.61	Russian Federation	e.cogat.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
180.166.131.142	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
79.176.76.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.197	Russian Federation	e.himush.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
176.13.13.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.191.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.176	Russian Federation	test.ncore.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
132.64.25.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.39	Russian Federation	mobile.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
62.90.202.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.175.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.71.122	147.237.72.156	United States	aman.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
93.157.86.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.8.45	Russian Federation	e.eitan.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
31.168.64.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
195.245.205.76	147.237.0.35	Russian Federation	akaws.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
82.166.148.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.216	Russian Federation	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.0.15	Russian Federation	kosher-kravi.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
81.218.251.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.166.131.142	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
79.181.151.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.199	Russian Federation	e.nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
176.13.230.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
78.11.173.46	147.237.77.216	Poland	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.177	Russian Federation	ncore.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
141.226.147.179	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
62.210.250.111	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
109.65.62.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.71.251	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.8.46	Russian Federation	e.chinuch.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
37.142.185.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
31.154.81.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.8.14	Russian Federation	e.orchot.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
84.95.85.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-05-2016-10:09:33 to 09-05-2016-11:09:33

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.49.85.55	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	688
1.201.102.11	Korea, Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	204
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
1.201.102.11	Korea, Republic of	147.237.76.86	navy.idf.il	SYN Attack		monitor	24
2.55.155.108	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.230.5	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
5.22.134.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
62.0.210.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.246.139.56	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
83.142.230.136	United Kingdom	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.253.196.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
132.64.207.193	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
82.81.46.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.81.46.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.3.147.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
95.97.231.135	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
36.80.102.233	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.55.45.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
81.218.176.47	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
201.46.55.42	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
83.142.230.136	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
141.226.218.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
83.142.230.136	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
46.19.86.209	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.160.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.46.38.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
80.178.203.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
85.65.114.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.230	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.225	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-05-2016-10:09:33 to 09-05-2016-11:09:33

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.201.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
2.53.146.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
2.55.170.16	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	25
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
123.152.67.211	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 123.152.67.211	Block	17
123.152.67.211	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 123.152.67.211	Block	17
213.57.165.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	7
123.152.67.211	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
123.152.67.211	China	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	6
109.253.204.246	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	6
194.54.168.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
37.26.146.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.138.215.36	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	3
176.13.231.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.54.168.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/9/	Block	3
176.13.243.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.13.219	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
109.253.230.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
93.172.151.103	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	2
194.54.168.65	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 194.54.168.65	Block	2
80.246.138.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.179.210.180	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
46.117.60.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
123.152.67.211	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/index.asp	Block	1
37.26.147.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.64.144.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
79.181.3.90	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
204.79.180.81	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
62.219.164.254	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.42	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication	Block	1
45.79.71.122	United States	147.237.72.156	aman.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
77.138.30.213	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
37.26.148.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.97.44	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.183.44.223	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/cityofficers	Block	1
207.46.13.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/gallery/	None	1
66.85.185.81	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
176.13.9.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
107.199.63.120	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
5.22.134.166	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.86.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
37.142.185.235	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
109.253.196.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.146.95	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - 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

09-05-2016-10:09:33 to 09-05-2016-11:09:33