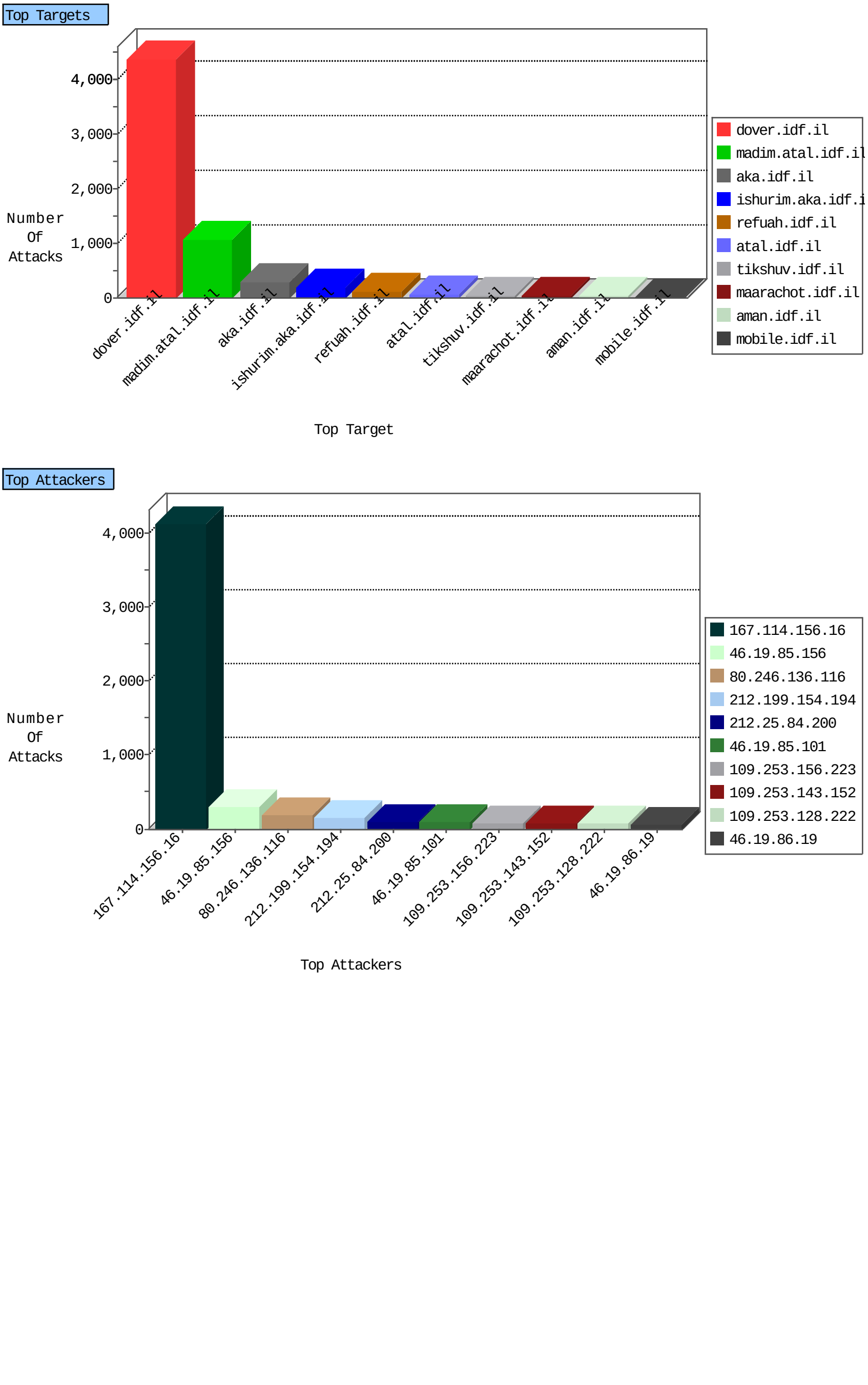
04-17-2016-09:04:07 to 04-17-2016-10:04:07

IDF Under Attack Daily Report



04-17-2016-09:04:07 to 04-17-2016-10:04:07

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	4125
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	886
167.220.196.89	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
104.148.71.133	United States	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
104.148.71.133	United States	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.40.4.195	Russian Federation	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.74	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
152.178.71.13	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.40.4.195	Russian Federation	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.78	United States	147.237.8.45	e.eitan.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
184.105.139.102	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.78	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1

04-17-2016-09:04:07 to 04-17-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
87.70.90.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
37.142.72.227	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-17-2016-09:04:07 to 04-17-2016-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.187.34.14	147.237.77.170	France	maarachot.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.85.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.68.75.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.4.79.76	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.146.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.4.79.76	147.237.76.31	Germany	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.36.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.84.148.3	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.144.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.114.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.12.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.109.207.230	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.19.85.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.130	147.237.0.17	Romania	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.253.211.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.4.79.76	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.67.38.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
43.249.219.123	147.237.76.198	India	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
84.111.15.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.207.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.62.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.100.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.131.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.130	147.237.0.33	Romania	idf.il	ET SCAN NMAP -sS window 1024	1

04-17-2016-09:04:07 to 04-17-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.25.84.200	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	90
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	71
62.90.221.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.183.212.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
79.181.183.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.90.142.51	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
5.102.232.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.149.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.90.142.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
2.53.8.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.66.107	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.159	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
109.64.221.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.26.146.145	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.9.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.161.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.64.221.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.9.119	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.137.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.64.221.26	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
185.120.125.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.53.63.71	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.60.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.33	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.240.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.33	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	5
5.29.109.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.48.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
93.158.152.25	Russian Federation	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
82.80.53.27	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
2.55.188.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.150.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.191.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.33	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
62.90.142.51	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.254.76	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.135.102.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.208.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.191.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.150.201.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-17-2016-09:04:07 to 04-17-2016-10:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.179.147.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.170.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.18.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-17-2016-09:04:07 to 04-17-2016-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	300
80.246.136.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	199
46.19.85.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
109.253.156.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
109.253.143.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
109.253.128.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
2.53.36.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
176.13.20.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
37.187.34.14	France	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 37.187.34.14	Block	22
2.55.12.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.85.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
37.187.34.14	France	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	11
37.26.148.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.53.36.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
199.30.16.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
95.86.72.55	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.149.187	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
199.30.25.46	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.224.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.171.241	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	3
109.253.224.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.27	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.123	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.143.232.123	Block	2
199.30.24.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.133.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.144.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.151.62.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	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	1
37.26.148.168	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
132.73.205.110	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.206	Israel	147.237.0.34	tikshuv.idf.il	Distributed Malformed URL	Block	1
213.244.116.250	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4466.jpg	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9686-he/refuah.aspx	Block	1
31.168.103.115	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.103.115	Block	1
157.55.39.188	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/www.rabanut-downloads.webs.com	Block	1
62.90.221.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
87.68.7.167	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
46.19.85.135	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 4d45 in URL	Block	1
212.199.244.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl33 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
188.143.232.123	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
2.55.168.206	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 2.55.168.206 (Open Mode)	None	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-17-2016-09:04:07 to 04-17-2016-10:04:07