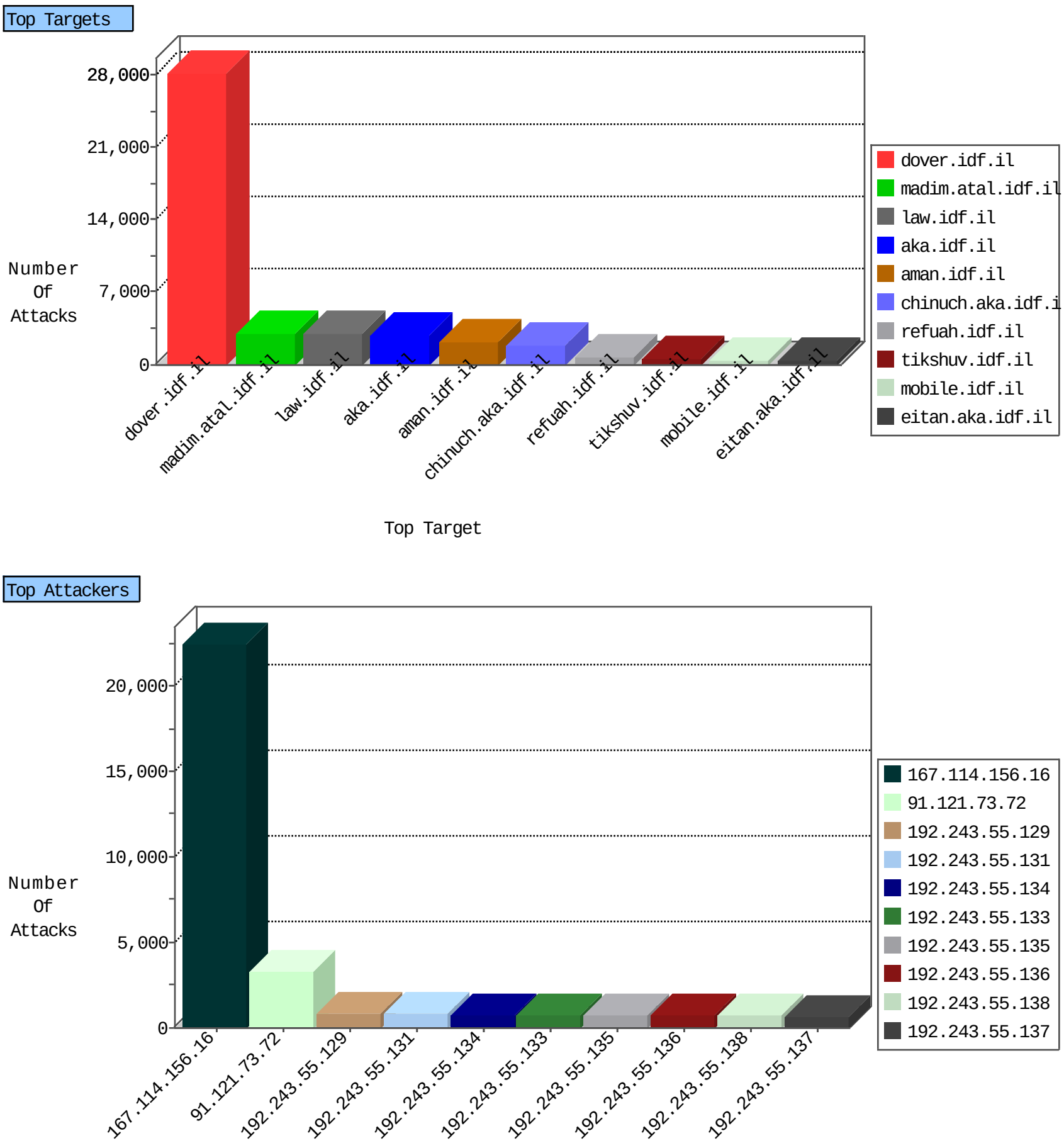
03-11-2016 to 03-12-2016

IDF Under Attack
Daily Report



03-11-2016 to 03-12-2016

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	DOS-Tool-SwitchbladG	dest-reset	90028
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	641
46.19.86.43	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	54
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	34
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	16
82.145.209.162	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
82.145.211.179	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
82.145.209.105	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
82.145.220.103	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
82.145.218.105	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
79.177.175.217	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
82.145.222.28	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
82.145.221.234	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
82.145.221.86	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
8.37.237.151	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	6
109.64.36.1	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.221.255	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
84.111.125.88	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.223.60	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
8.37.237.151	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4
212.88.63.206	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
114.55.25.14	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	4
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-traf1	forward	3
71.6.158.166	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets_Con_Limit	drop	3
109.67.210.1	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	2
120.26.199.234	China	147.237.0.34	tikshuv.idf.il	L4 Source or Dest Port Zero	drop	2
204.42.253.2	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	2
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
115.239.228.10	China	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Http	drop	2
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	2
125.26.17.253	Thailand	147.237.77.226	www.chamatz.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

03-11-2016 to 03-12-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	42
79.181.198.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	26
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.120.173.118	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
83.130.108.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
207.232.46.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
84.111.38.183	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
98.19.222.133	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
149.50.94.14	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
85.250.112.25	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
109.67.113.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.65.170.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.65.11.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
176.13.10.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.71.99.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.71.100.76	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.54.144.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
79.181.218.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.78.239.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.253.216.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.i	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.26.149.204	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.66.16.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.29.32.142	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
70.68.224.173	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
89.138.176.28	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.163.148.58	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
193.200.80.26	United Kingdom	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
152.115.70.227	Denmark	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
94.73.150.148	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.120.55.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.67.144.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
197.35.20.2	Egypt	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	4
209.15.196.170	Canada	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.120.91.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.179.32.28	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
209.15.196.170	Canada	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.192.50	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.77	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
216.185.43.135	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
23.91.70.119	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3

03-11-2016 to 03-12-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.185	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	192
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	96
98.19.222.133	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	31
193.200.80.26	147.237.76.86	United Kingdom	navy.idf.il	SQL Injection - Select From	12
152.115.70.227	147.237.76.42	Denmark	refuah.idf.il	SQL Injection - Select From	12
209.15.196.170	147.237.77.216	Canada	dover.idf.il	SQL Injection - Select From	10
23.91.70.119	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
177.185.192.50	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
94.73.150.148	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	6
23.91.70.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
177.185.192.77	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	5
176.13.7.106	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
109.253.204.65	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
103.228.130.69	147.237.77.216	China	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	4
103.228.130.69	147.237.77.216	China	dover.idf.il	SERVER-IIS multiple extension code execution attempt	4
103.228.130.69	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	4
70.68.224.173	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	4
80.246.130.156	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	3
89.163.146.236	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
193.105.134.220	147.237.76.30	Sweden	himush.idf.il	ET SCAN NMAP -sS window 1024	2
89.163.146.236	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.93.121	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
207.225.131.141	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.182.170.38	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	2
167.114.172.229	147.237.77.216	Canada	dover.idf.il	SERVER-APACHE Apache mod_proxy reverse proxy information disclosure attempt	2
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	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
93.189.26.18	147.237.8.27	Austria	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
178.63.11.208	147.237.8.27	Germany	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
89.163.146.236	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.35	Germany	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
89.163.146.236	147.237.0.33	Germany	idf.il	ET SCAN Potential VNC Scan 5900-5920	2
61.182.170.38	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	2
89.163.146.236	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.93.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
61.182.170.38	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.159	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
218.57.11.7	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
122.116.206.72	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
52.33.159.204	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
189.254.90.133	147.237.77.235	Mexico	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
173.224.117.146	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.25.81	147.237.0.33	France	idf.il	ET SCAN NMAP -sS window 2048	1
199.101.186.245	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
181.214.92.181	147.237.77.121	Chile	e.navy.idf.il	ET SCAN Potential SSH Scan	1

03-11-2016 to 03-12-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.73.72	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1139
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	865
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	671
91.121.73.72	France	147.237.72.156	aman.idf.il	SYN Attack		reject	441
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	166
176.13.14.244	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	150
2.54.25.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	150
79.176.21.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	134
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	128
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	128
79.176.21.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	125
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	120
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	118
91.121.73.72	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	118
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	117
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	115
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	114
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	108
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	108
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	105
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	105
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	104
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	100
85.64.37.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	94
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	94
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	93
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	92
79.179.148.217	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	89
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	89
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	84
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	82
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	81
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	81
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	80
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	79
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	79
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	78
91.121.73.72	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	77
176.13.14.244	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	75
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	74
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	74
192.243.55.136	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	73
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	73
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	73
62.128.48.50	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	71
107.77.70.118	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	503
109.66.32.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	427
79.183.203.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	196
5.29.248.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	157
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
87.71.29.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
89.139.225.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
84.108.182.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
87.70.78.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
176.13.14.244	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	81
109.253.144.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
176.13.19.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
176.13.18.27	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	49
46.19.86.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
103.228.130.69	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 103.228.130.69	Block	46
149.88.177.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
176.13.10.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
2.54.158.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
173.208.136.170	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	40
173.208.136.170	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	40
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	38
103.228.130.69	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	37
109.253.159.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
212.34.12.100	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.12.100	Block	23
212.34.12.100	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.12.100	Block	23
79.180.71.39	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.71.39	Block	22
176.13.10.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.19.85.114	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.114	Block	17
46.19.86.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
212.34.12.100	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.12.100	Block	14
79.183.17.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
79.183.229.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	12
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	12
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.7	Block	11
109.64.238.116	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	11
83.130.108.116	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	10
109.65.26.65	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.65.26.65	Block	10
80.84.1.10	Satellite Provide	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
5.29.148.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
173.208.136.170	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	8
109.64.238.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
131.253.25.154	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	7
173.208.136.170	United States	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	7

03-11-2016 to 03-12-2016