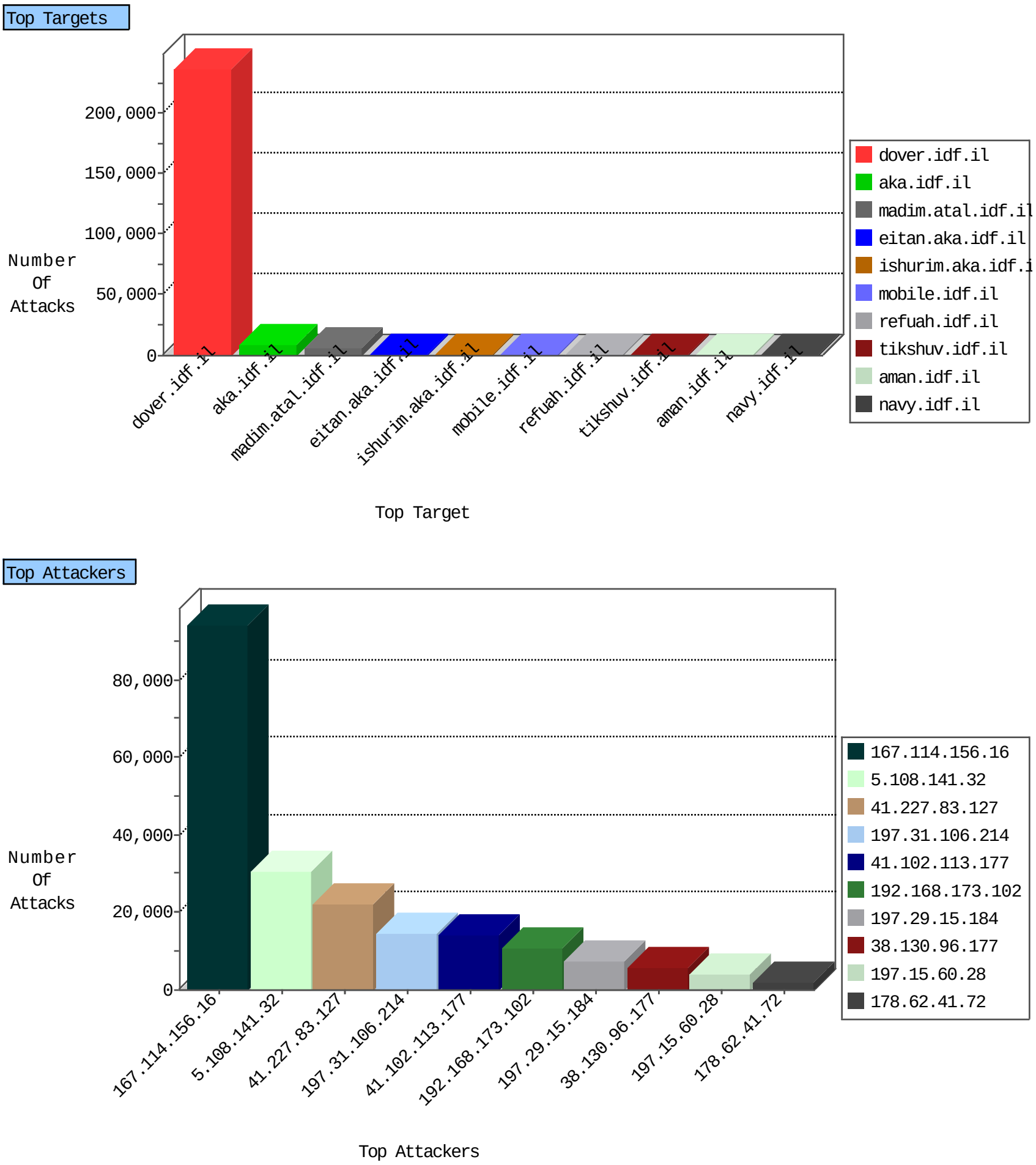
04-10-2016 to 04-11-2016

IDF Under Attack
Daily Report



04-10-2016 to 04-11-2016

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.i	Block_Ip_Web_In	drop	94334
41.227.83.127	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	5207
197.31.106.214	Tunisia	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	3985
197.15.60.28	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3707
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	3547
197.29.15.184	Tunisia	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3420
38.130.96.177	United States	147.237.77.216	dover.idf.i	HTTP-MISC-DoS-GoodBye-30	dest-reset	3146
109.67.228.35	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2796
188.161.30.85	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	1734
2.54.128.118	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1214
41.227.83.127	Tunisia	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	1208
197.15.9.10	Tunisia	147.237.77.216	dover.idf.i	HTTP-MISC-Acunetix-product3	dest-reset	1119
46.19.86.61	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1110
197.31.106.214	Tunisia	147.237.77.216	dover.idf.i	Invalid TCP Flags	drop	1108
212.143.142.56	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1091
5.56.16.192	Anonymous Proxy	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	981
154.98.30.15	Sudan	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	979
79.177.85.153	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	881
197.28.190.16	Tunisia	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	850
41.111.2.130	Algeria	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	807
197.29.15.184	Tunisia	147.237.77.216	dover.idf.i	Invalid TCP Flags	drop	713
47.17.214.150	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	692
41.227.83.127	Tunisia	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	635
212.179.90.106	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	594
154.98.30.15	Sudan	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	584
105.108.71.184	Algeria	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	549
188.161.30.85	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	529
141.255.146.110	Netherlands	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	442
197.29.15.184	Tunisia	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	440
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	411
0.0.0.0		147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	309
41.224.66.164	Tunisia	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	289
192.249.66.247	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	287
41.107.97.131	Algeria	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	240
46.121.96.110	Israel	147.237.77.216	dover.idf.i	HTTP-POST-Segmented-DoS	dest-reset	233
207.46.13.192	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	213
38.130.96.177	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	213
45.56.73.98	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	208
84.228.234.180	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	201
199.115.115.210	United States	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	178
0.0.0.0		147.237.77.216	dover.idf.i	HTTP Page Flood Attack	drop	177
156.205.95.137	Egypt	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	150
109.64.233.196	Israel	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	144
156.203.85.136	Egypt	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	135
109.64.233.196	Israel	147.237.77.216	dover.idf.i	HTTP-MISC-DoS-GoodBye-30	dest-reset	130
37.237.210.133	Iraq	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	118
84.111.226.10	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	108
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
38.130.96.177	United States	147.237.77.216	dover.idf.i	Block_Udp_All_Nets	drop	101
38.130.96.177	United States	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	90

04-10-2016 to 04-11-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	25
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
62.219.137.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	17
149.78.240.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
212.150.5.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
149.88.229.120	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
80.74.110.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
37.142.68.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
81.218.57.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	10
87.71.66.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
79.182.22.159	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
105.157.150.208	Morocco	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	9
62.219.44.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
109.67.170.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
149.78.206.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.54.129.111	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.176.89.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	6
91.230.243.165	United Kingdom	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
185.3.144.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
69.30.219.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	5
37.142.245.132	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
109.253.141.224	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
77.125.95.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
77.126.142.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.176.86.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.144.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
212.143.103.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.181.6.178	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.52.130.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.164.20	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
87.71.1.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.10.204	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.117.101.255	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
41.105.244.242	Algeria	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	4
212.150.125.221	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
41.254.5.129	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	3
198.204.230.114	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	3
66.249.93.109	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
31.168.123.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
65.55.210.151	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.53.23.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
83.149.126.98	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2

04-10-2016 to 04-11-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.9.81	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	822
45.56.73.98	147.237.77.216	United States	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	703
66.249.93.115	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	125
66.249.78.15	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	117
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	67
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	66
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER /etc/passwd	59
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP phpThumb fltr[] parameter remote command execution attempt	26
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	25
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP awstats access	23
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ETPRO WEB_SERVER PHP Open Flash Charts File Upload Attempt	21
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP WEB-INF access	16
156.203.85.136	147.237.77.216	Egypt	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	12
79.178.18.67	147.237.72.167	Israel	ishurim.aka.idf.i	POLICY-OTHER TCP packet with urgent flag attempt	12
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP webalizer access	9
41.254.5.129	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP login.htm access	9
199.115.115.210	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	9
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER webalizer access	9
41.254.5.129	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SERVER-WEBAPP admin.php access	7
197.15.60.28	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP admin.php access	5
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER auto_prepend_file PHP config option in uri	5
5.8.45.251	147.237.77.216	Chile	dover.idf.il	SQL Injection - Select From	5
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER allow_url_include PHP config option in uri	5
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP PHP-CGI remote file include attempt	5
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attemp	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP JBoss JMX console access attempt	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER suhosin.simulation PHP config option in uri	4
197.15.60.28	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP login.htm access	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER open_basedir PHP config option in uri	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	4
199.203.84.80	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP TRACE attempt	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER safe_mode PHP config option in uri	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER disable_functions PHP config option in uri	4
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP client negative Content-Length attempt	4
199.115.117.199	147.237.77.216	United States	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
85.203.18.254	147.237.77.216	Sweden	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	3
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt	3
197.41.73.83	147.237.77.216	Egypt	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	3
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET SCAN DEBUG Method Request with Command	3
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	2
80.82.78.38	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP JBoss web console access attempt	2
88.204.187.90	147.237.77.235	Kazakstan	sviva.idf.il	ET SCAN NMAP -sS window 4096	2
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	2
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	ET SCAN Apache mod_proxy Reverse Proxy Exposure 2	2
88.204.187.90	147.237.77.235	Kazakstan	sviva.idf.il	ET SCAN NMAP -f -sS	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
41.105.244.242	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	2
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2

04-10-2016 to 04-11-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25379
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18712
41.102.113.177	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14026
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	7120
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5906
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5403
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	3803
38.130.96.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2595
197.15.60.28	Tunisia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2121
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		reject	2037
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1998
38.130.96.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1959
196.121.32.248	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1733
197.28.190.16	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1568
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	drop		drop	1532
41.105.244.242	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1314
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	1269
197.15.60.28	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1020
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1005
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	836
141.255.146.110	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	809
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	684
141.255.153.12	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	624
109.64.233.196	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	520
165.51.217.168	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	519
46.19.85.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	493
46.116.180.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	469
45.56.73.98	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	465
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	424
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	drop		drop	413
141.255.153.12	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	384
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	367
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	322
141.255.153.12	Netherlands	147.237.77.216	dover.idf.il	SYN Attack		reject	313
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	303
154.98.30.15	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	302
217.78.62.175	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	297
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	288
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		reject	279
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	273
195.60.232.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	260
41.107.97.131	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	256
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
197.15.60.28	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	209
41.227.83.127	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	202
41.107.97.131	Algeria	147.237.77.216	dover.idf.il	drop		drop	194
149.88.62.22	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	176
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	158
79.178.22.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
109.67.228.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	151

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	851
109.64.171.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	317
176.13.14.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	311
109.253.136.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	303
197.15.60.28	Tunisia	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning V1	Block	262
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	221
109.253.193.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	216
95.35.82.239	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.35.82.239	Block	201
176.13.18.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	193
2.54.128.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	187
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	162
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	160
2.55.20.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	147
2.54.165.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
2.53.39.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	123
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
41.254.5.129	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.254.5.129	Block	103
2.53.40.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
41.254.5.129	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	101
85.64.210.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
176.13.7.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
2.55.55.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
2.53.15.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	89
109.253.212.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
194.90.66.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
62.90.131.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
109.253.202.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 95.187.96.157	Block	79
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 95.187.96.157	Block	79
95.187.96.157	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 95.187.96.157	Block	79
37.26.148.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
45.56.73.98	United States	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	78
45.56.73.98	United States	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	78
45.56.73.98	United States	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	78
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
197.15.60.28	Tunisia	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 197.15.60.28	Block	72
197.15.60.28	Tunisia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 197.15.60.28	Block	72
197.15.60.28	Tunisia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 197.15.60.28	Block	72
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	72
46.19.86.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
109.253.138.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
46.19.85.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
46.19.86.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
185.32.179.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
109.253.144.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
84.228.229.33	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	55
2.52.190.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
46.19.86.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54

04-10-2016 to 04-11-2016