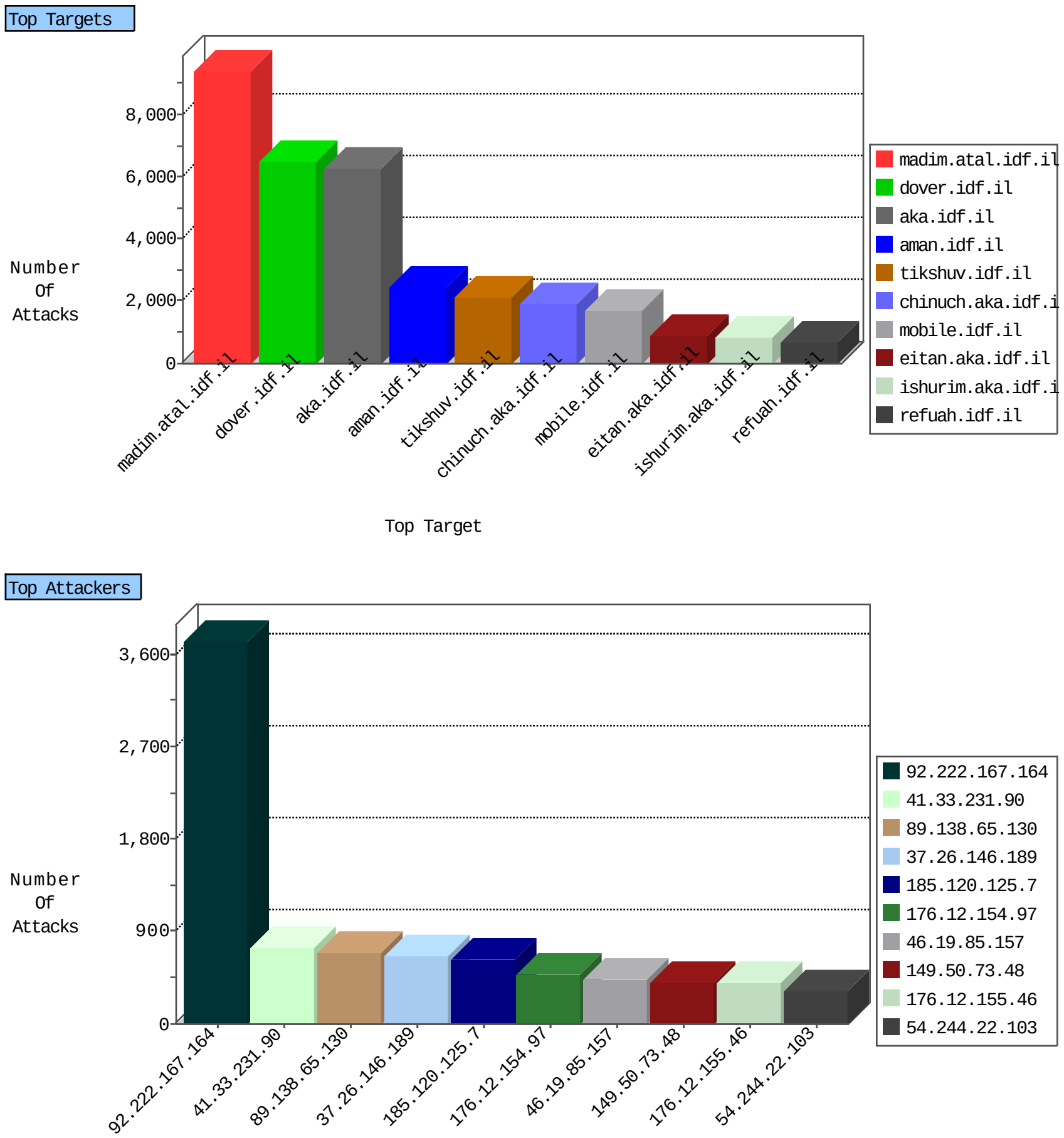
02-02-2016 to 02-03-2016

IDF Under Attack Daily Report



02-02-2016 to 02-03-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.0.14.217	Europe	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2116
70.192.135.153	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1709
37.26.148.252	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1013
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	994
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	797
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	296
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	237
176.12.155.80	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	226
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
91.231.192.149	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	81
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	74
46.19.86.69	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
79.178.229.125	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	40
91.231.192.149	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	31
208.109.97.62	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	23
77.255.195.72	Poland	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	22
80.246.136.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
91.202.171.11	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
80.215.135.219	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.66.192.180	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.109.112.43	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.67.26.72	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.166.137.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.54.170.217	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
79.181.56.211	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
168.235.196.172	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
213.8.204.80	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
125.164.39.13	Indonesia	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
164.138.122.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.19.85.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.64.175.178	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.116.205.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.245	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
109.66.135.112	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.246.130.163	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
2.52.179.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
200.53.9.113	Brazil	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
124.232.137.57	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
46.19.86.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

02-02-2016 to 02-03-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.105.122.30	Saudi Arabia	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	8
93.169.180.90	Romania	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	3
151.80.31.151	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
208.52.161.99	United States	147.237.72.156	aman.idf.il	C003: HTTP: phpMyAdmin access	Block	1
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
208.52.161.99	United States	147.237.77.226	www.chamatz.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
93.123.108.83	Bulgaria	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
208.52.161.99	United States	147.237.76.39	mobile.meitav.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.0.15	kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
148.251.50.49	Germany	147.237.76.86	navy.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
62.210.190.10	France	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1
208.52.161.99	United States	147.237.77.170	maarachot.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.72.166	aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.77.233	atal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.42	refuah.idf.il	C003: HTTP: phpMyAdmin access	Block	1
51.255.162.163	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
208.52.161.99	United States	147.237.0.17	m.my-kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
151.80.31.111	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.225.135	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
208.52.161.99	United States	147.237.77.176	matpash.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.72.167	ishurim.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
151.80.31.154	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
208.52.161.99	United States	147.237.77.234	halag.idf.il	C003: HTTP: phpMyAdmin access	Block	1
94.102.153.58	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
51.255.207.27	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
208.52.161.99	United States	147.237.76.147	chinuch.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.0.19	madim.atal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
151.80.31.150	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
85.136.227.77	Spain	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
208.52.161.99	United States	147.237.77.205	prisha.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.30	himush.idf.il	C003: HTTP: phpMyAdmin access	Block	1
162.210.196.130	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
208.52.161.99	United States	147.237.77.235	sviva.idf.il	C003: HTTP: phpMyAdmin access	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
52.26.202.58	United States	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
208.52.161.99	United States	147.237.76.200	eitan.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.0.34	tikshuv.idf.il	C003: HTTP: phpMyAdmin access	Block	1
151.80.31.150	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
208.52.161.99	United States	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.99	United States	147.237.76.31	nakchal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
36.110.147.103	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.169	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
216.17.111.245	United States	147.237.77.19	law-forum.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
118.238.227.101	Japan	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
52.32.210.122	United States	147.237.72.166	aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
208.52.161.99	United States	147.237.77.74	law.idf.il	C003: HTTP: phpMyAdmin access	Block	1

02-02-2016 to 02-03-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	68
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	21
37.105.122.30	147.237.77.216	Saudi Arabia	dover.idf.il	SQL Injection - Select From	11
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	9
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
52.35.178.67	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	8
37.105.122.30	147.237.77.216	Saudi Arabia	dover.idf.il	GPL WEB_SERVER /etc/passwd	6
192.115.67.2	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
178.162.208.141	147.237.77.233	Germany	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
118.238.227.101	147.237.76.42	Japan	refuah.idf.il	SQL Injection - Select From	4
80.246.133.70	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
37.237.154.56	147.237.77.216	Iraq	dover.idf.il	ET SCAN NMAP -sA (2)	4
85.136.227.77	147.237.77.74	Spain	law.idf.il	SQL Injection - Select From	3
94.102.153.58	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	3
62.210.225.135	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	3
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
84.111.48.244	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
199.191.56.187	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	2
199.191.56.187	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	2
209.126.116.147	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
217.21.7.6	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
84.228.222.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.139	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
37.8.24.236	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
46.31.103.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
2.54.30.246	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
195.60.232.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
178.162.208.141	147.237.76.30	Germany	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.88.101	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	2
168.1.28.110	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.170	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
62.90.131.234	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.75.130	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
183.12.148.73	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
209.126.116.147	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	2
66.249.66.72	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
54.157.215.29	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2

02-02-2016 to 02-03-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
92.222.167.164	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1862
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1262
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	722
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	554
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	414
109.65.17.107	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	209
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	208
37.26.146.150	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	186
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
79.177.209.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	126
168.235.196.172	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	121
92.225.45.103	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	108
79.178.36.101	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
79.182.96.166	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
185.92.76.69		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
31.168.29.185	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	90
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	88
41.254.2.32	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
2.54.182.108	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
37.26.148.214	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
46.19.85.5	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	79
46.19.85.116	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	74
99.237.104.94	Canada	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	70
212.235.103.203	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	69
79.182.171.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
84.94.121.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	56
46.19.85.105	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
80.246.133.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
195.154.116.56	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	51
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
46.19.85.120	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	48
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	48
37.26.147.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
51.36.104.173	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
141.0.14.217	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
80.246.136.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	41
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
46.19.85.33	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
185.3.144.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
77.125.151.131	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
80.246.130.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
213.55.111.1	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
85.130.194.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.246.133.246	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
37.26.149.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 89.138.65.130	Block	374
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	371
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	262
149.50.73.48	United States	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	255
176.12.154.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	244
176.12.154.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	218
176.12.155.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	216
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 89.138.65.130	Block	212
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.146.189	Block	186
46.210.193.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
79.181.246.103	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.246.103	Block	155
5.22.129.99	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	152
99.237.104.94	Canada	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
176.12.155.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	141
176.12.154.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
149.50.73.48	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	140
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	140
37.142.64.93	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.96	Block	129
176.12.154.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	117
37.26.146.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
176.12.155.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.50	Block	111
149.88.59.64	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.59.64	Block	111
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
82.81.29.135	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
176.12.155.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.12.155.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.12.154.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
46.19.86.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
80.246.137.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
176.12.154.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
80.246.136.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
149.88.152.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
176.12.155.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
176.12.154.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
176.12.155.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
176.12.154.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
176.12.155.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
2.52.183.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
176.12.154.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
79.182.59.196	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.59.196	Block	74
176.12.155.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	73