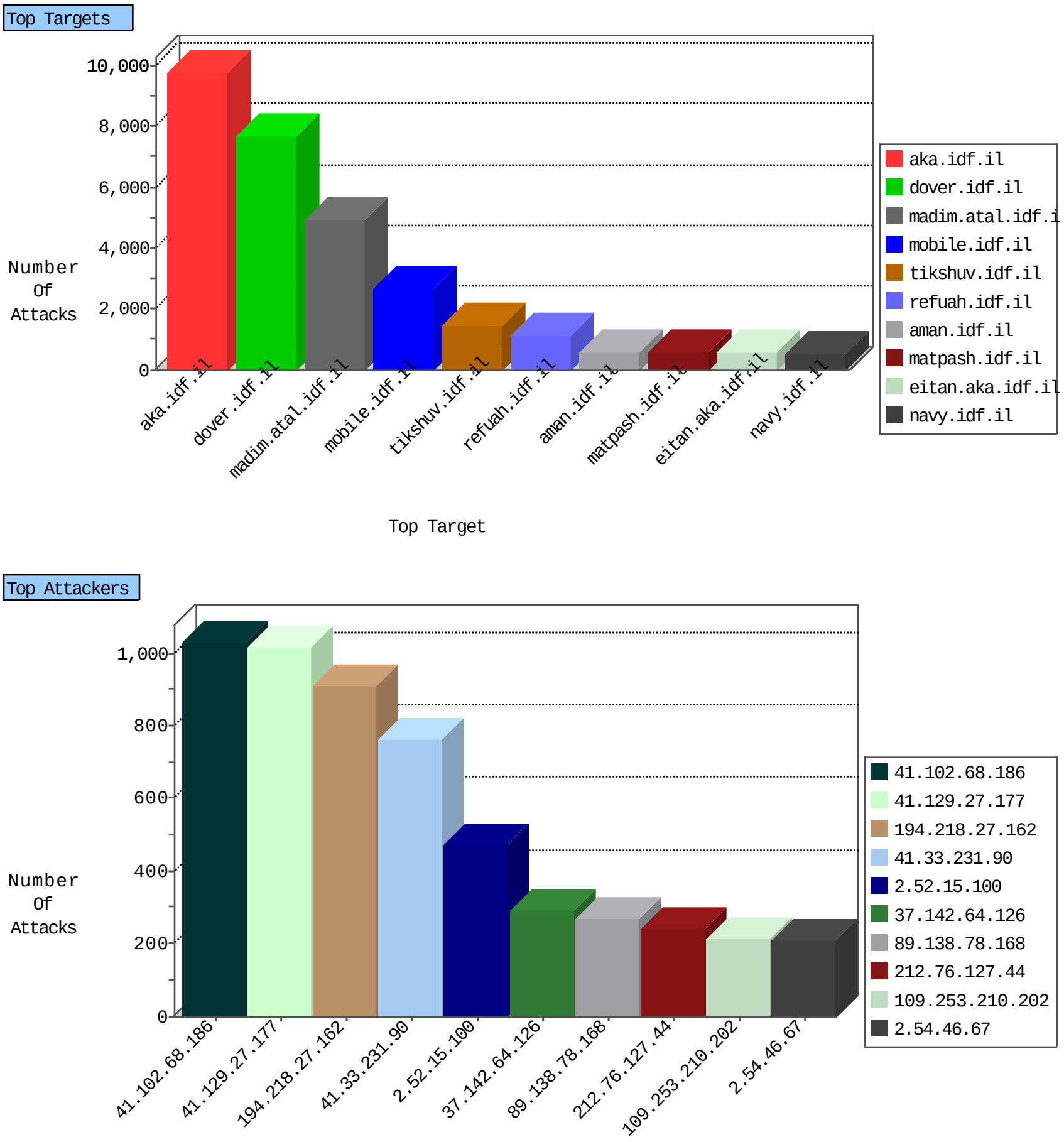
02-28-2016 to 02-29-2016

IDF Under Attack Daily Report



02-28-2016 to 02-29-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.109.97.62	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	220514
37.26.148.129	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	26051
37.26.148.178	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	22826
41.102.68.186	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	375
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	282
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	114
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
197.117.169.65	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	97
79.181.132.139	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	27
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	16
79.181.132.139	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	15
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	14
82.145.219.113	Europe	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	14
82.145.219.100	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
82.145.211.199	Europe	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
62.0.34.177	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
82.145.208.241	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
79.176.52.14	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
182.140.167.188	China	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	6
147.235.8.31	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	6
82.145.208.174	Europe	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	6
79.178.206.135	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
212.179.54.237	Israel	147.237.77.216	dover.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
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
193.104.77.4	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.208.74	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
178.33.179.251	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
197.117.169.65	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	4
79.180.204.181	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.145.208.74	Europe	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	3
79.178.151.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.181.132.139	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.65.104.164	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.118.64.213	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
79.180.120.16	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
149.88.106.86	Israel	147.237.72.166	aka.idf.il	Anomaly-TCP-shortheader	dest-reset	3
41.102.68.186	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
173.252.75.116	United States	147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	2
41.102.68.186	Algeria	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	2
124.130.148.202	China	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	2
115.239.228.10	China	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.26.149.242	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2

02-28-2016 to 02-29-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.51.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	44
192.114.91.213	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	37
66.249.81.196	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	28
106.120.173.124	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
46.19.86.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	22
85.65.93.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	22
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
46.19.85.90	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
61.135.189.121	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
94.188.158.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
46.116.143.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
66.249.81.199	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
46.117.144.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
91.121.101.78	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	16
66.249.81.202	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
217.194.206.30	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
5.28.157.67	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
212.179.42.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.179.114.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
5.29.84.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
94.159.157.78	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.246.130.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
77.126.164.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.179.12.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
89.138.169.64	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
85.64.99.12	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
2.54.145.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	10
37.26.147.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
176.13.11.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
5.29.78.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
213.57.169.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
188.120.148.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.163.88	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.70.31.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.176.233.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.235.31.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.230.37.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.142.68.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.3.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.68.77	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.250.42.203	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.235.64.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.10.243	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
66.249.81.202	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.25.84.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8

02-28-2016 to 02-29-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.167	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	168
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	68
41.129.27.177	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP adminlogin access	8
41.129.27.177	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP admin.php access	7
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.154.58.230	147.237.77.176	France	matpash.idf.il	SERVER-WEBAPP yabb access	6
41.129.27.177	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP login.htm access	4
82.80.89.41	147.237.72.166	Israel	aka.idf.il	GPL SCAN nmap TCP	4
66.249.81.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	4
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
54.82.8.196	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
66.249.75.223	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
93.172.231.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
185.130.5.173	147.237.0.34		tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.102.9.28	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
80.246.137.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
74.208.153.47	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	2
202.79.243.160	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	2
37.26.147.187	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
213.57.155.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.75.231	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
188.120.135.12	147.237.72.166	Israel	aka.idf.il	GPL SCAN nmap TCP	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
78.229.100.85	147.237.77.216	France	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.173	147.237.0.33		idf.il	ET SCAN Potential VNC Scan 5900-5920	2
104.192.0.19	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
79.180.210.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
160.179.189.54	147.237.77.216		dover.idf.il	SERVER-WEBAPP admin.php access	2
66.249.93.32	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
151.11.201.3	147.237.77.61	Italy	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	2
149.88.12.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
195.154.58.230	147.237.77.176	France	matpash.idf.il	SERVER-WEBAPP modules.php access	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
104.192.0.19	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.95.76.194	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
84.229.148.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.180.198.185	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
79.176.160.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.182.58.195	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.178.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
12.9.106.137	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
213.8.204.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
149.78.183.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.27.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016 to 02-29-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	733
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	608
41.102.68.186	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	533
2.52.15.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	471
41.129.27.177	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	395
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	302
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	192
213.57.93.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	188
109.64.0.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	142
46.210.151.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	117
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	106
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
185.120.126.67		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	91
37.26.146.152	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
192.124.249.2		147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	82
192.124.249.2		147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	80
41.102.68.186	Algeria	147.237.77.216	dover.idf.il	drop		drop	76
194.30.134.180	Cyprus	147.237.72.166	aka.idf.il	drop	SAM rule	drop	76
80.246.130.191	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	72
95.35.204.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
185.32.179.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	53
217.132.119.0	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
5.102.195.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
195.154.173.103	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	48
109.253.194.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
85.130.252.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.85.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
185.120.126.67		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	45
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
79.179.9.115	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
213.8.204.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
176.13.21.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
62.90.201.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
109.253.132.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	37
147.161.14.79	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
46.19.85.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
77.125.98.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
46.19.85.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	33
212.34.23.120	Jordan	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	33
62.0.34.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
212.25.105.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
212.29.225.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

02-28-2016 to 02-29-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.129.27.177	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.129.27.177	Block	373
37.142.64.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	291
89.138.78.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	248
109.253.210.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	211
2.54.174.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	202
2.54.46.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	202
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	178
2.54.32.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	150
37.26.148.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
2.54.132.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
37.26.149.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
80.246.137.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
41.129.27.177	Egypt	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.129.27.177	Block	105
109.253.150.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
160.179.189.54		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 160.179.189.54	Block	98
46.19.86.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
41.129.27.177	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	96
197.27.77.181	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.27.77.181	Block	93
176.13.18.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
46.19.86.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
79.182.184.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
79.181.236.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
80.246.136.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
37.26.149.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
2.54.169.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
2.54.129.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
109.253.209.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
109.253.146.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
109.253.156.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
176.13.1.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
176.13.22.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
2.52.47.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
109.253.131.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
176.13.10.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
46.116.177.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
80.246.136.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
2.54.22.75	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	45
109.253.145.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
37.26.149.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
176.13.9.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.121.195.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
2.54.188.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
176.13.12.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
37.26.149.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37

02-28-2016 to 02-29-2016