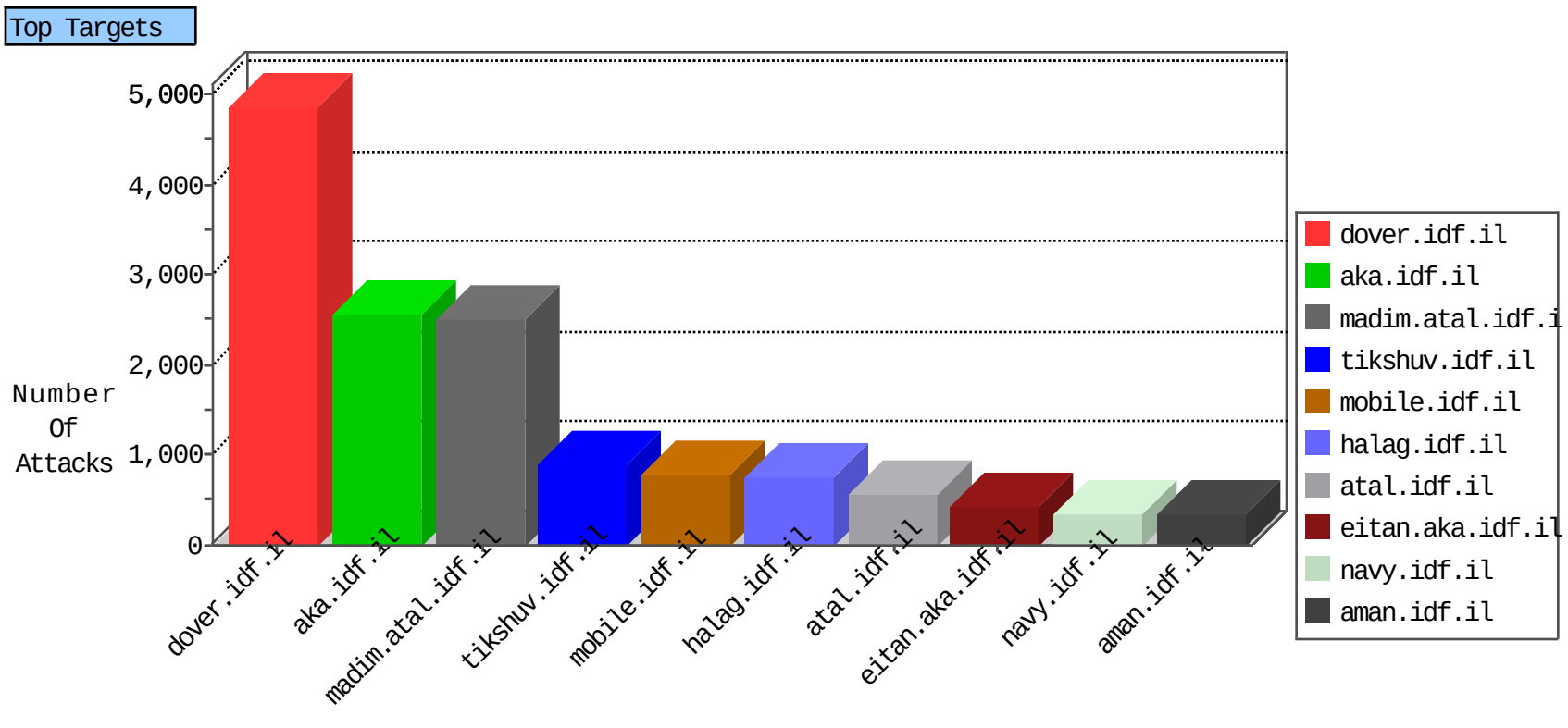
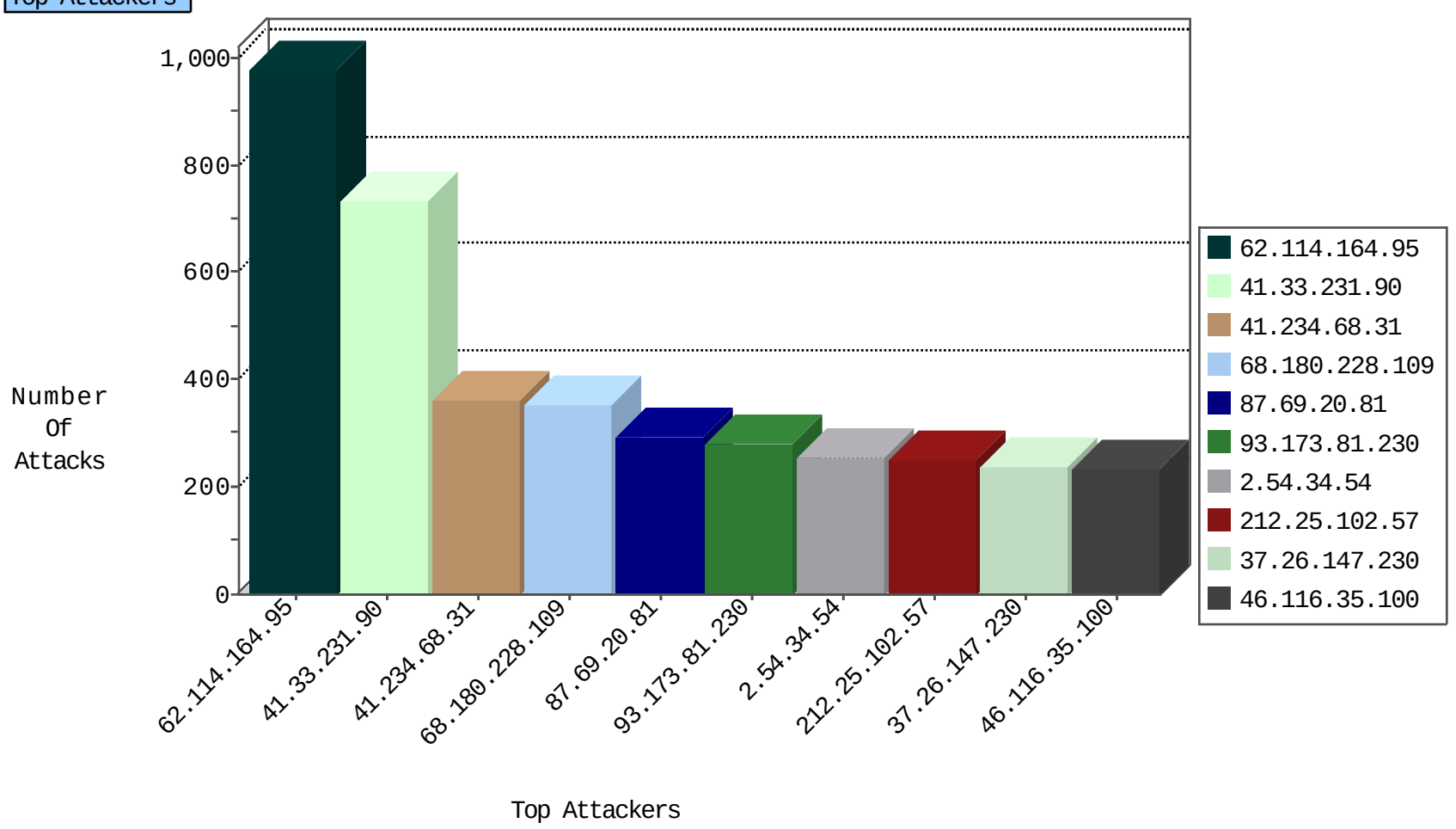
02-26-2016 to 02-27-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-26-2016 to 02-27-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.31	United States	147.237.76.147	chinuch.aka.idf.il	TCP handshake violation, first packet not syn	drop	76876
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3090
41.234.68.31	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2166
66.249.66.36	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	115
64.233.172.155	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	40
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	22
82.145.218.131	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
82.145.211.118	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	15
82.145.209.100	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	12
82.145.219.90	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
141.255.155.40	Netherlands	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	10
46.135.154.20	Czech Republic	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
79.182.128.122	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
41.234.68.31	Egypt	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
82.145.222.45	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
84.108.152.18	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	4
109.65.49.86	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.177.128.172	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
70.39.185.221	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
8.37.237.162	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
109.65.49.86	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.177.230.247	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.65.49.86	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
79.177.128.172	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	2
222.188.100.102	China	147.237.0.33	idf.il	Invalid TCP Flags	drop	2
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
79.177.230.247	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
70.39.185.221	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
82.79.205.124	Romania	147.237.72.156	aman.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
31.206.69.70	Turkey	147.237.72.166	aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
8.37.237.162	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	2
82.145.218.95	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
125.75.206.153	China	147.237.8.27	e.madim.atal.idf.il	Invalid TCP Flags	drop	2
61.178.192.219	China	147.237.77.19	law-forum.idf.il	Invalid TCP Flags	drop	2
109.200.216.22	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1

02-26-2016 to 02-27-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.160.179	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	32
123.126.113.102	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	22
80.246.130.149	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	18
149.78.136.236	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	18
207.46.13.145	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	18
149.88.188.253	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	18
68.180.228.109	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	18
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	16
79.176.105.95	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	15
109.253.146.183	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	14
46.120.190.202	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	13
109.66.211.232	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	13
85.64.21.135	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	12
46.120.36.93	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	12
85.64.224.33	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.177.135.127	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	12
61.135.189.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	11
217.194.206.43	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	10
37.26.147.193	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.50.74.119	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.201.246	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
77.125.143.63	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
157.55.39.92	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.204.49	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.51.172	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	7
84.108.153.86	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	6
37.26.146.133	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.241	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.66.7.192	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	6
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
46.120.2.93	Israel	147.237.0.34	tikshuv.idf.i	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	4
85.65.167.150	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.57.130.46	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
85.64.201.143	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.11.82	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.116.4.77	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.29.9.42	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.23.38	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
95.86.64.79	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
77.243.189.243	Europe	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	4
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
85.65.6.241	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.142.217.131	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.120.250.120	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	3
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	3
88.217.35.95	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
79.176.50.107	Israel	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.81	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2

02-26-2016 to 02-27-2016

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	93
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	37
80.246.130.135	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	25
80.246.133.214	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	11
37.26.147.230	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
185.32.179.142	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
46.60.30.111	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	4
185.95.255.42	147.237.76.30		himush.idf.il	ET SCAN NMAP -sA (2)	4
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	3
37.46.39.27	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
198.54.90.200	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
74.143.224.18	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
185.95.255.42	147.237.76.86		navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.152	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.158	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
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
80.80.109.85	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	2
218.246.0.97	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
79.176.168.157	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
109.253.202.131	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
94.102.48.193	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	2
37.142.118.230	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.46.39.27	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
93.174.91.29	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	2
84.228.6.210	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.174	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
176.13.15.28	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
80.80.109.85	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
211.154.163.110	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	2
82.205.35.253	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
91.228.126.61	147.237.72.166	Israel	aka.idf.il	Tehila - Perl LWP with fake user agent	2
41.234.68.31	147.237.77.216	Egypt	dover.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.75.239	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
66.102.9.17	147.237.72.167	United States	ishurim.aka.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
169.54.233.124	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
104.215.89.20	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.79.104	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.206	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
50.60.153.98	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
118.165.7.106	147.237.76.197	Taiwan	e.himush.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
62.210.189.248	147.237.77.74	France	law.idf.il	ET SCAN Potential SSH Scan	1
204.101.135.203	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.138.70.153	147.237.0.33	Sweden	idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

02-26-2016 to 02-27-2016

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	652
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	338
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	336
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	332
93.173.81.230	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	262
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	244
79.178.104.59	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	214
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	204
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
79.183.65.178	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	138
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	94
70.39.185.221	Satellite Provide	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	72
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	69
2.52.179.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	65
213.57.180.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	drop		drop	51
185.3.146.94	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	51
188.120.148.105	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
149.50.74.119	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
5.22.131.87	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	38
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
70.114.238.87	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.234.68.31	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
62.114.164.95	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
213.8.90.143	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	monitor	33
109.253.138.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
82.166.42.84	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
128.199.233.32	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	29
141.0.14.148	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
80.246.133.3	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
210.117.199.102	Korea, Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
70.39.185.221	Satellite Provide	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
107.167.98.43	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
176.13.4.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
85.65.63.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
2.52.56.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.28.167.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	24
87.68.243.30	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
185.120.126.24		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24

02-26-2016 to 02-27-2016

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.20.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	292
2.54.34.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	252
46.116.35.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	232
37.26.147.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	225
82.166.61.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	179
2.54.63.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	156
79.180.57.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
80.246.137.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
77.125.255.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
85.65.106.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	73
176.13.16.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
93.173.236.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
109.253.147.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
5.29.46.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	30
176.13.17.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
109.253.207.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
109.67.11.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
37.26.147.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
2.54.142.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
80.246.136.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
80.250.149.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	15
149.78.235.234	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 149.78.235.234	Block	14
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	13
79.177.144.43	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.144.43	Block	13
109.160.131.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
80.246.130.49	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	11
109.67.14.59	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.67.14.59	Block	11
46.121.214.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
109.253.220.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
79.176.221.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.120.51.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.138.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
65.55.210.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
2.54.180.6	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	8
185.120.126.24		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	7
176.13.4.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
157.55.39.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
37.26.147.230	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	7
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	7
79.177.144.43	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	7
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	7
79.177.182.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
195.91.212.123	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6

02-26-2016 to 02-27-2016