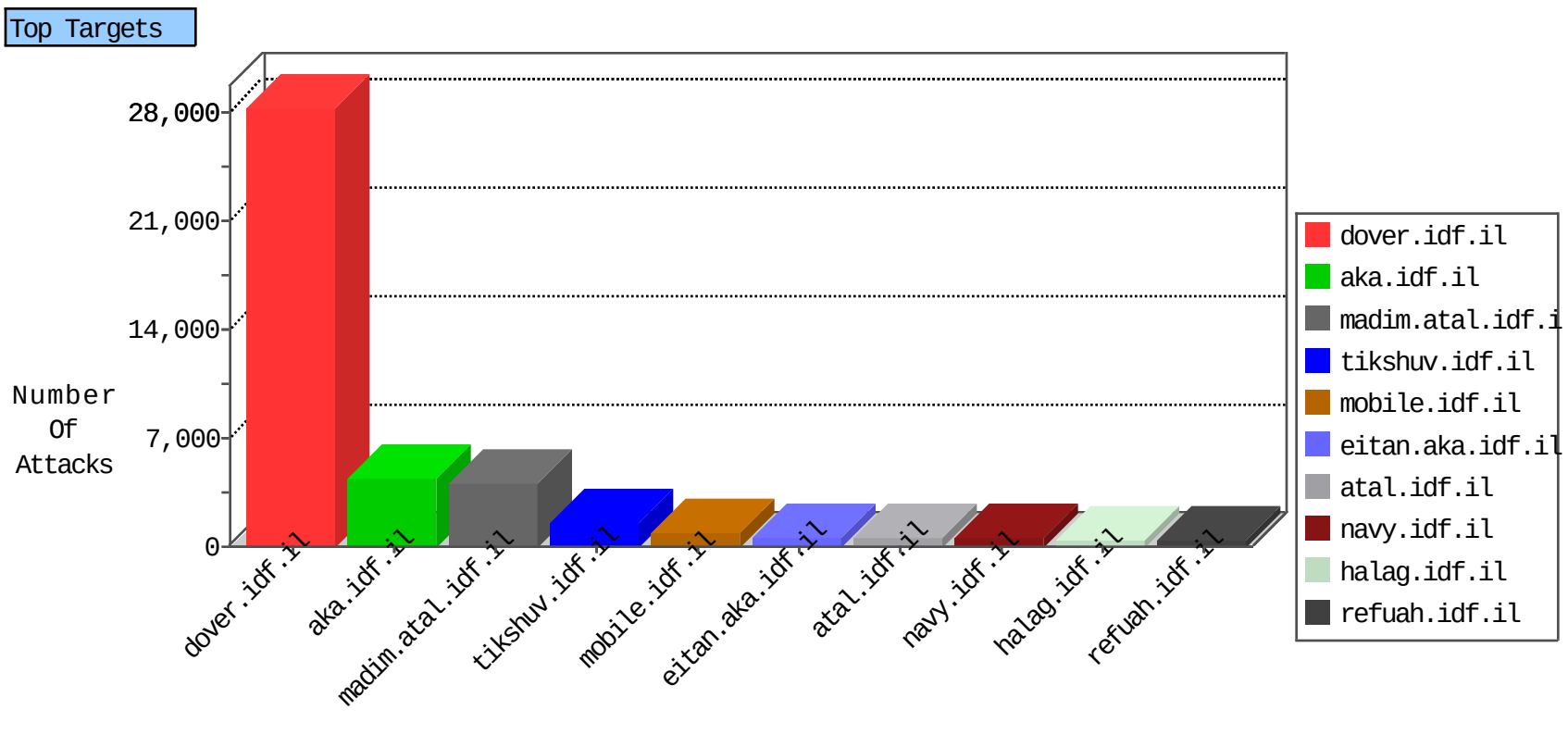
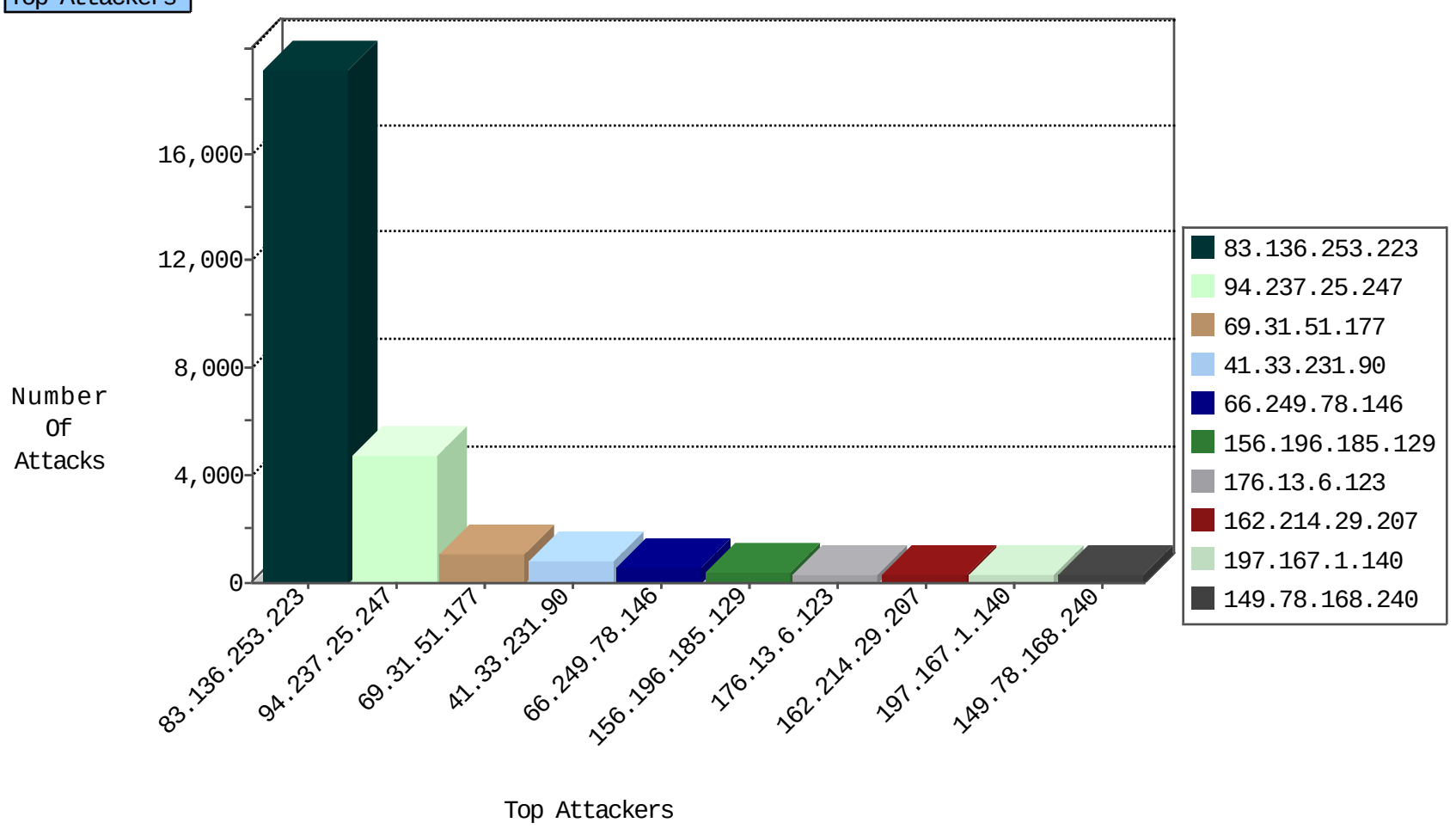
02-27-2016 to 02-28-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-27-2016 to 02-28-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	42705
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	10362
66.249.93.67	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	9614
66.249.93.123	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3162
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	649
94.237.25.247	Finland	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	394
94.237.25.247	Finland	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	345
156.196.185.129		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	225
156.196.185.129		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	184
0.0.0.0		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	182
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	160
82.145.216.148	Europe	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	106
93.172.253.171	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	105
46.120.39.155	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	73
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	36
84.111.125.88	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	36
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	21
156.197.161.254		147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	20
82.145.217.247	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	16
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	14
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	12
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
94.237.25.247	Finland	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	12
82.145.209.16	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
156.197.161.254		147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
94.237.25.247	Finland	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	8
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	7
82.145.218.138	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
82.145.219.64	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
82.145.220.169	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.180.120.16	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	6
82.145.211.203	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.180.120.16	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
105.154.69.57	Morocco	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	6
82.145.223.56	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	6
66.249.93.127	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5
184.167.154.90	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	4
82.145.208.75	Europe	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
105.154.69.57	Morocco	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4
66.151.244.102	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	3
46.188.42.117	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
168.235.197.107	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.177.230.247	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
125.75.206.156	China	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	2
168.235.197.107	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2

02-27-2016 to 02-28-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	23
61.135.189.121	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	21
123.126.113.102	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
80.246.133.255	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
162.214.29.207	United States	147.237.72.166	aka.idf.il	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	10
46.121.63.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
213.57.155.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
45.35.110.136		147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	10
162.214.29.207	United States	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	10
37.26.147.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
213.57.63.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.69.245.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.183.182.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.76.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.108.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
93.172.62.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.117.154.174	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.94.41.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.140.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.64.5.161	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.6	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
77.127.163.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.177.135.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.78.5.211	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.228.197.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
185.3.147.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.180.120.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
207.46.13.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
84.108.154.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.178.122.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
46.19.85.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
37.26.149.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.121.105.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.66.121.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
87.71.24.30	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.239.205.207	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
109.67.149.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.142.152.185	Israel	147.237.0.34	tikshuv.idf.il	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
77.125.80.157	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
195.154.185.20	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
107.150.56.254	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	3
51.255.65.75	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	3
51.255.65.59	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	3

02-27-2016 to 02-28-2016

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	94
162.214.29.207	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	76
162.214.29.207	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP Mambo upload.php access	40
80.246.136.24	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	12
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
188.120.148.142	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	6
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
66.102.9.81	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	3
95.45.254.123	147.237.77.216	Ireland	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
85.113.96.235	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
59.46.193.114	147.237.77.74	China	law.idf.il	GPL SCAN nmap TCP	2
217.78.62.77	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	2
94.102.48.193	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
66.102.9.28	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
194.63.140.74	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	2
210.115.184.234	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
194.63.140.74	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
46.60.29.159	147.237.77.74	Palestinian Territory, Occupied	law.idf.il	ET SCAN NMAP -sA (2)	2
218.24.171.223	147.237.77.74	China	law.idf.il	GPL SCAN nmap TCP	2
37.26.149.185	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
194.63.140.74	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	2
113.53.106.72	147.237.76.86	Thailand	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.27.85.28	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential SSH Scan	1
2.54.169.34	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
194.63.140.74	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.76.38	Italy	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.193	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
180.191.105.107	147.237.0.34	Philippines	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
191.248.83.29	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.141.236.69	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.167	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
40.78.62.82	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
201.166.217.148	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
169.54.233.118	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.255.65.207	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.69.71	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
223.4.174.30	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.71.251.11	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.91.29	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
49.205.32.125	147.237.0.34	India	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-27-2016 to 02-28-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18642
94.237.25.247	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4564
69.31.51.177	Anonymous Proxy	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	962
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	804
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	304
109.64.16.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	163
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
79.182.237.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
105.154.69.57	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
105.154.69.57	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
69.31.51.177	Anonymous Proxy	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	100
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	96
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	95
37.46.41.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
46.188.42.117	Russian Federation	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	73
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	71
180.253.246.121	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	68
2.54.193.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	63
5.29.203.122	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
94.237.25.247	Finland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	58
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	54
83.248.57.21	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
46.32.170.122	Azerbaijan	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
83.136.253.223	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	45
31.210.187.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
2.54.193.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
109.65.142.7	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
5.22.134.234	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
95.86.119.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
79.181.30.187	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
2.54.193.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
37.46.39.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
85.64.248.27	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
79.183.59.37	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
46.116.199.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.76.124.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
177.1.170.11	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
217.21.7.173	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
213.57.140.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
45.35.110.136		147.237.77.216	dover.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
89.138.109.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
79.178.236.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
77.125.152.234	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	305
149.78.168.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	273
80.246.136.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	239
109.64.125.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	198
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	188
37.142.64.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	170
2.54.38.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	163
176.13.12.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
2.54.138.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
31.154.190.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
109.253.208.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
2.54.166.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
46.116.9.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
109.253.146.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
80.246.139.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
41.224.80.140	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	87
109.226.28.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	85
109.66.219.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
46.19.86.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
162.214.29.207	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	75
162.214.29.207	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 162.214.29.207	Block	73
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
46.120.170.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
109.160.131.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.65.242.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	49
109.66.193.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.86.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
185.32.179.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.86.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
93.173.188.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
79.178.30.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
5.102.254.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.177.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
45.35.110.136		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.35.110.136	Block	25
185.32.179.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
109.253.203.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.86.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
162.214.29.207	United States	147.237.72.166	aka.idf.il	Multiple signatures from 162.214.29.207	Block	18
2.54.191.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	17
41.224.80.140	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	15
41.224.80.140	Tunisia	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 41.224.80.140	Block	14
95.35.95.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14

02-27-2016 to 02-28-2016