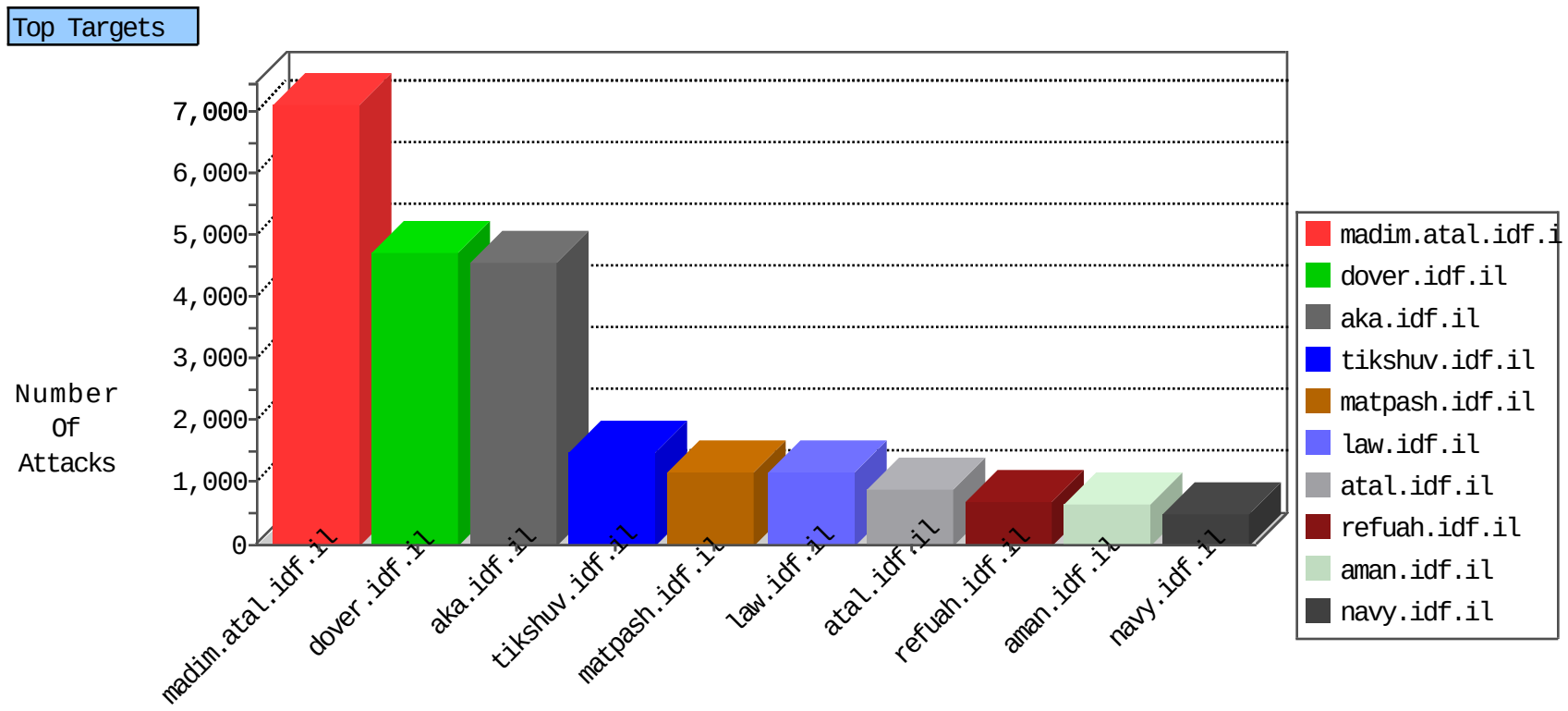
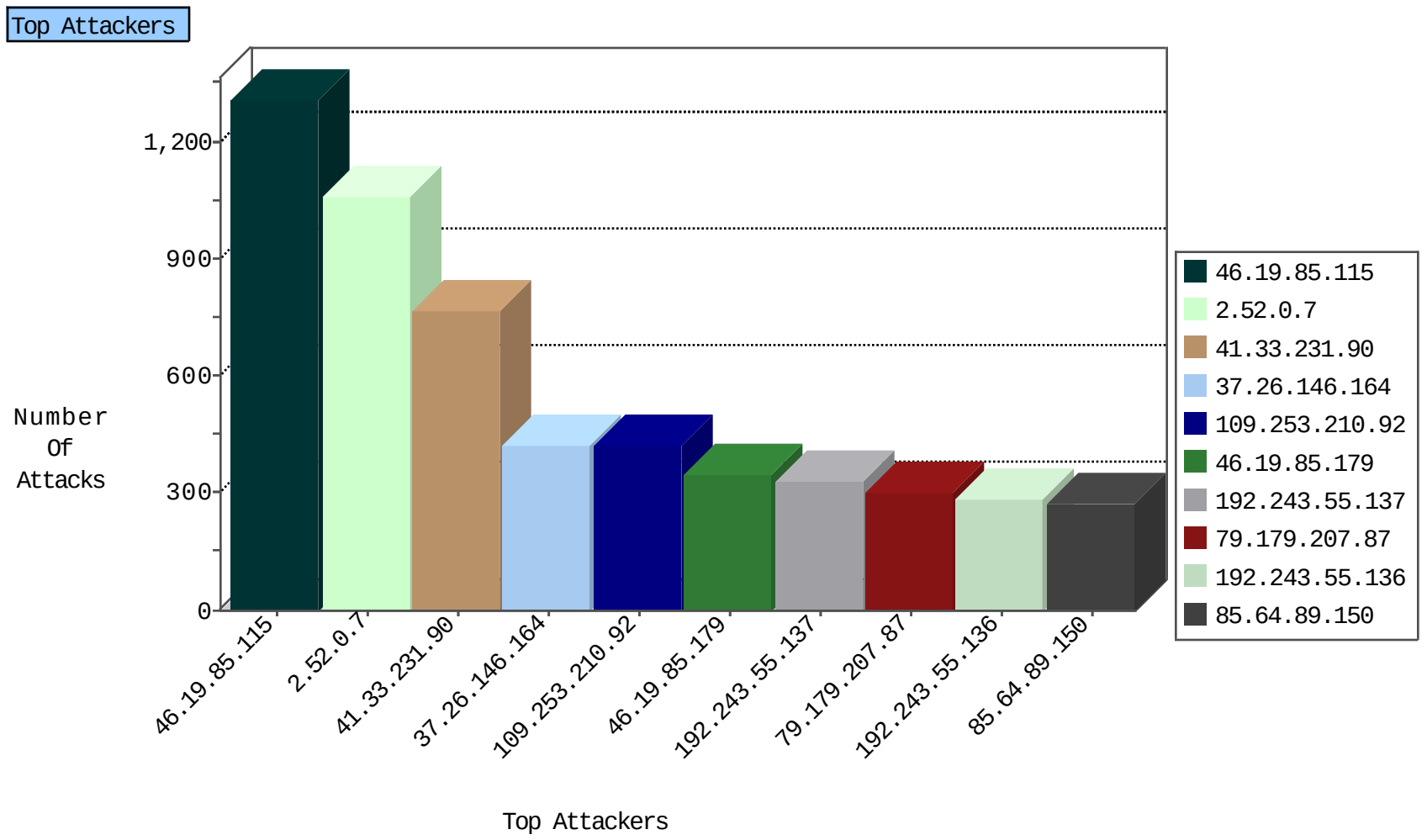
02-18-2016 to 02-19-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-18-2016 to 02-19-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.207.87	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	242
66.249.66.39	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	221
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
212.199.154.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
79.179.207.87	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
37.26.146.192	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
62.117.59.18	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
79.177.236.233	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
109.67.10.142	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
90.148.10.87	Saudi Arabia	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	6
79.179.207.87	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	6
84.111.125.88	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.146.215	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
82.145.222.38	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
91.221.58.27	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
115.239.228.10	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	4
167.114.133.208	Canada	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	3
198.84.193.7	Canada	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
195.212.29.177	Europe	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
69.171.230.106	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.46.189	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.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
40.77.167.38	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.130.5.201		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2
217.55.235.79	Egypt	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	2
185.94.111.1		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
222.186.21.181	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
217.172.189.11	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.94.111.1		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
195.212.29.177	Europe	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.130.5.201		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
185.130.5.201		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
217.172.189.11	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	2
115.236.75.201	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.130.5.224		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2

02-18-2016 to 02-19-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	41
138.134.102.16	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	30
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	26
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	25
81.218.70.243	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
46.117.62.87	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	22
84.109.39.112	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
79.183.33.59	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
212.179.79.150	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
138.134.102.15	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
109.65.72.158	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
82.81.4.54	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
79.181.200.159	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
85.64.249.42	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
74.63.228.226	United States	147.237.77.226	www.chamatz.aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	9
79.178.70.114	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
188.120.134.202	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
46.19.85.33	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
5.102.206.203	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
87.69.146.42	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
149.88.146.149	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
69.167.186.64	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
216.10.220.154	Jamaica	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
74.63.228.226	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
84.111.81.211	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
5.29.78.38	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
87.69.140.114	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
84.111.138.219	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
194.56.215.218	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
149.78.166.204	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
164.138.122.127	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C1000228: HTTP: AhrefBot crawler	Block	6
109.67.165.182	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	6
195.154.185.20	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	6
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C1000228: HTTP: AhrefBot crawler	Block	5
84.110.192.161	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
213.8.145.99	Israel	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
69.167.186.64	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
85.65.38.41	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
74.63.228.226	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
193.200.80.26	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.137.81.122	Ireland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.234.228.90	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.29.118.44	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	4
177.185.194.45	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.137.81.122	Ireland	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

02-18-2016 to 02-19-2016

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	67
74.63.228.226	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	43
69.167.186.64	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	25
46.137.81.122	147.237.77.74	Ireland	law.idf.il	SQL Injection - Select From	17
185.95.255.42	147.237.76.30		himush.idf.il	ET SCAN NMAP -sA (2)	12
108.168.219.174	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	11
213.8.145.99	147.237.77.216	Israel	dover.idf.il	SQL Injection - Select From	11
193.200.80.26	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	9
66.76.174.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
108.168.219.174	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	7
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	7
195.140.210.83	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	7
80.246.133.236	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
203.171.41.47	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	5
70.89.127.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	5
195.234.228.90	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
177.185.194.45	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	4
80.246.133.37	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
188.64.169.106	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	3
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
222.186.21.181	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.74.104	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
72.27.221.77	147.237.76.44	Jamaica	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
80.246.133.6	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
218.246.0.97	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
66.102.9.6	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
188.64.169.106	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
115.236.75.201	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
70.89.127.78	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	2
192.198.151.45	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.0.107	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
107.191.102.245	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.93.67	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
94.102.48.193	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.180	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.102.9.17	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
188.64.169.106	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
62.0.24.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.243.181.86	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.206.232.19	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 3072	1
146.185.250.105	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.8.24	Romania	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
75.147.243.2	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.23.112.119	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.162	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

02-18-2016 to 02-19-2016

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	752
79.181.129.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	246
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	156
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	135
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	125
213.57.244.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	112
109.186.14.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	103
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	92
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	91
212.157.43.170	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	84
178.162.199.139	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	76
173.203.187.1	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	72
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	71
173.203.187.1	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
185.95.255.42		147.237.76.30	himush.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	67
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
185.95.255.42		147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	62
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.52.40.1	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	59
109.67.199.159	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
192.114.7.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	41
109.253.133.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
46.19.85.158	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	34
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
212.143.169.206	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
93.80.106.113	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	27
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	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
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK 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
79.177.9.173	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	26
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.0.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	675
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	501
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	441
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.164	Block	235
109.253.210.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	220
2.52.0.7	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.52.0.7	Block	217
109.253.210.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	196
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	195
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	175
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
2.52.0.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	167
84.94.41.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	160
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	150
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.115	Block	149
213.57.244.218	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	140
109.67.199.159	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	135
176.13.6.94	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	129
37.26.147.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
85.64.89.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	127
176.13.15.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
149.78.168.16	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	116
176.13.6.94	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.6.94	Block	110
84.94.41.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	107
85.64.89.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.13.4.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
188.120.154.246	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
2.52.170.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
176.13.9.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
37.26.147.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
2.54.10.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
109.253.210.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
2.54.7.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
84.111.49.2	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.111.49.2	Block	61
85.65.131.10	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
185.24.76.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
176.13.23.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
5.28.143.229	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.143.229	Block	57
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
185.32.179.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
79.176.186.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
109.253.201.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
176.13.4.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
82.81.194.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
176.13.19.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44