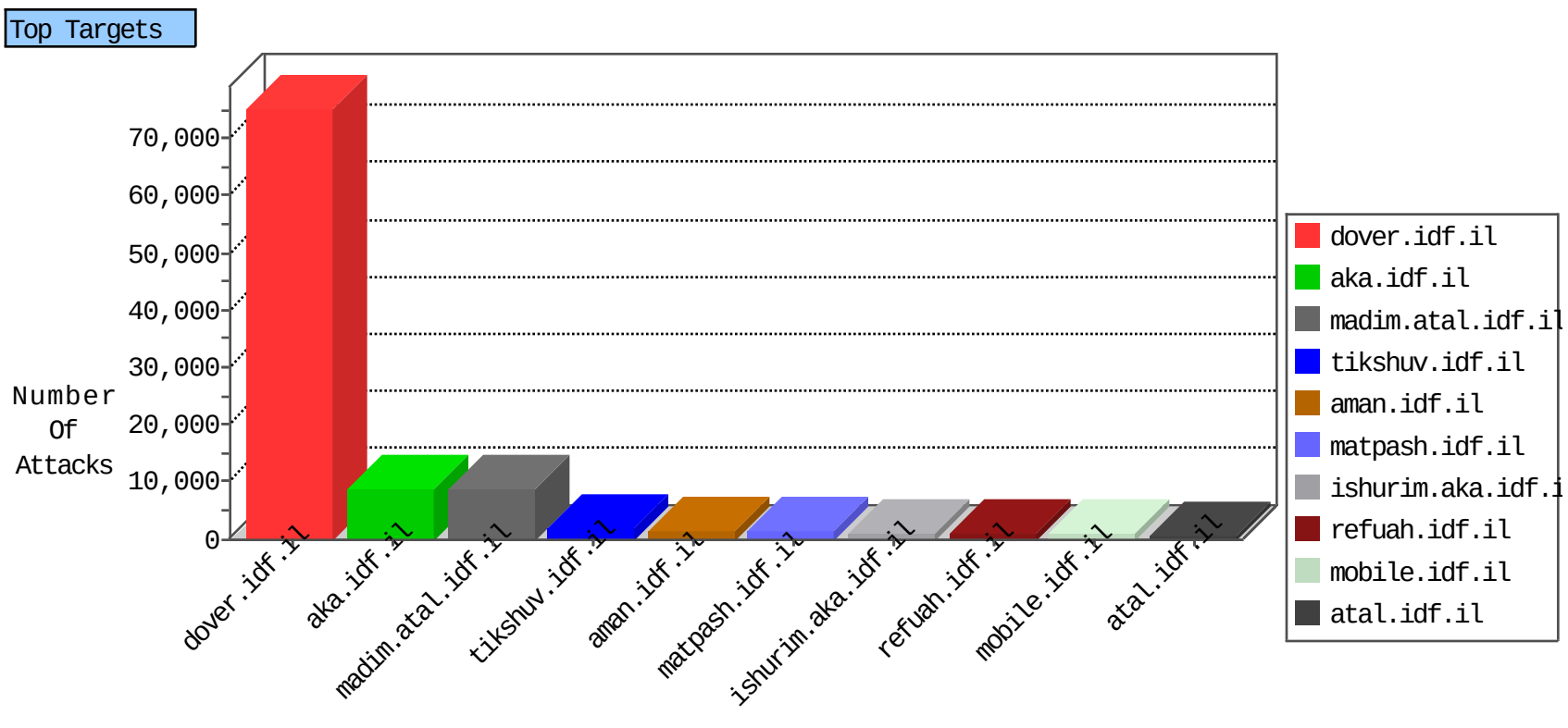
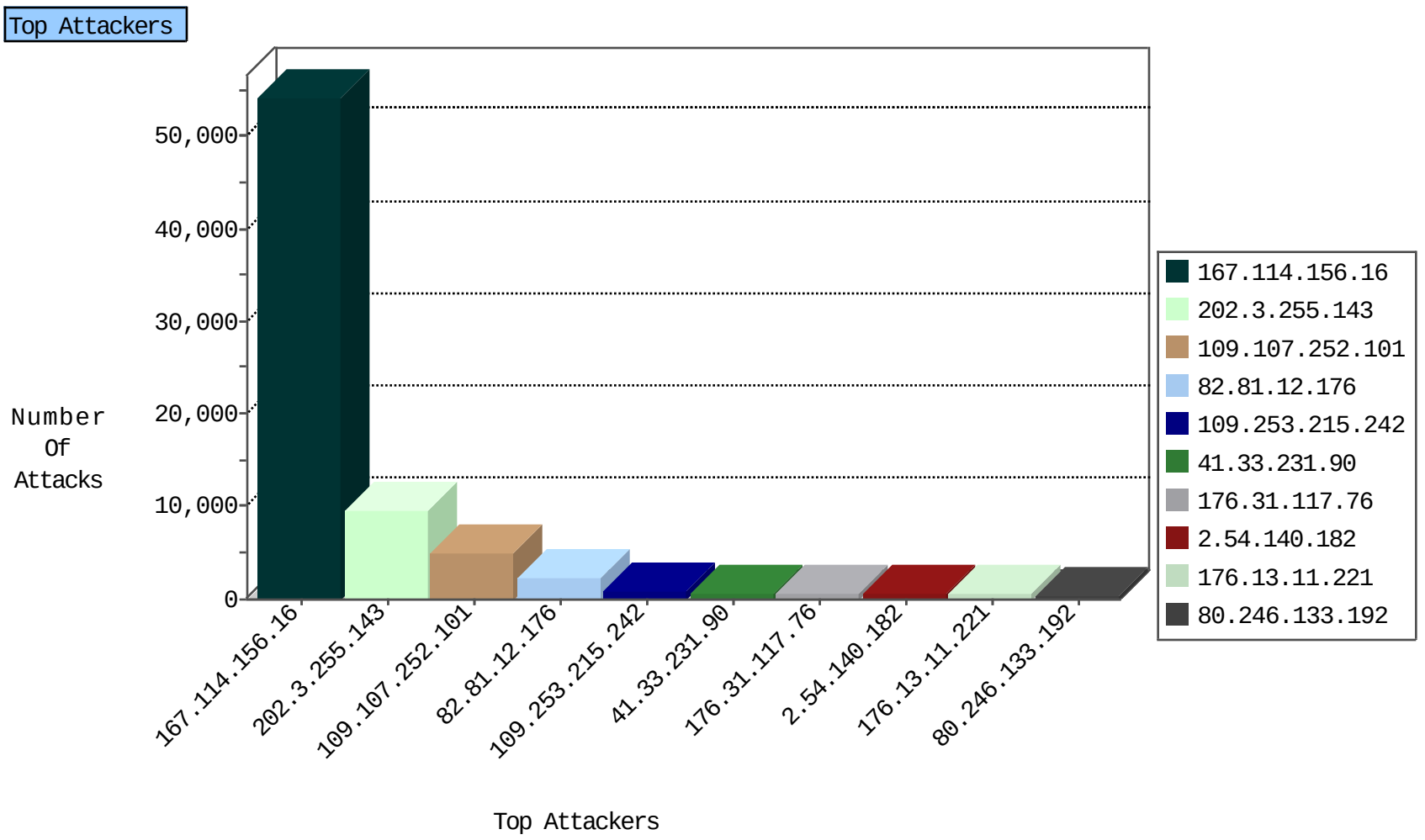
01-19-2016 to 01-20-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-19-2016 to 01-20-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	89386
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	TCP handshake violation, first packet not syn	drop	6282
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5116
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3595
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2413
106.38.241.106	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	900
37.26.146.205	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	515
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	471
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	415
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	276
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	208
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
79.180.161.175	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	48
212.179.37.196	Israel	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	42
66.249.64.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	25
79.180.121.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	19
66.249.69.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
31.17.11.120	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
41.200.100.52	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
78.188.47.90	Turkey	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
79.177.200.217	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.211.180	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.178.6.161	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
37.26.148.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
168.235.196.13	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
105.107.214.137	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
176.13.15.196	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.26.149.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.177.32.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.253.196.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.74.96.29	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	3
109.66.160.66	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
111.77.96.210	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
207.46.13.49	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.165.186	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
104.209.43.162	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.181.22.18	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
5.102.193.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.165.186	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3

01-19-2016 to 01-20-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	48
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	41
89.138.178.197	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	30
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	24
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	21
80.246.130.35	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	18
87.69.67.9	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	18
31.154.171.223	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	16
109.64.221.217	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	16
149.88.89.46	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	15
217.132.47.52	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	14
79.179.34.77	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	14
109.65.143.228	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	14
176.13.0.153	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	12
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	12
80.179.114.27	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	12
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	12
89.138.94.248	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	10
62.0.53.100	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	10
109.253.214.103	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
213.57.105.98	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
46.117.241.121	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
213.57.131.66	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
79.176.57.138	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
87.68.242.247	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
37.26.146.198	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
213.57.187.181	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
109.64.6.58	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
77.127.59.212	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
109.186.66.119	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	7
37.26.149.165	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
109.64.150.191	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
176.13.13.35	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.59	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
84.228.141.201	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
79.182.62.136	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.176	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
79.180.21.188	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	5
79.176.126.211	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	5
149.88.5.57	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
109.253.201.42	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
46.19.86.250	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
87.69.92.102	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
46.121.220.17	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
109.65.197.215	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
37.142.64.56	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
46.116.129.47	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
109.64.162.50	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	4

01-19-2016 to 01-20-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	8672
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	64
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	40
66.249.93.99	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	30
212.199.57.197	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	8
177.185.192.77	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	8
66.249.64.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	7
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	6
177.185.194.138	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	5
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	5
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	5
105.107.214.137	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	5
67.228.38.74	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	4
81.218.111.210	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
46.19.85.194	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
211.23.251.92	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	3
114.79.169.197	147.237.77.227	India	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
177.185.192.77	147.237.76.86	Brazil	navy.idf.il	SQL Injection - Select From	2
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
89.138.99.117	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.77	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
114.79.169.197	147.237.77.61	India	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.92	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
176.13.22.28	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
62.210.226.9	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	2
176.13.21.10	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
176.13.12.225	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
176.13.3.134	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
5.22.135.239	147.237.77.243	Israel	mobile.idf.il	INDICATOR-SCAN myscan	2
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
125.65.165.215	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.2	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.199.57.197	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
176.13.22.28	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
66.249.64.13	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
5.102.101.40	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
176.13.21.10	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
163.172.13.173	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
163.172.13.173	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	2
176.13.12.225	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.202	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
176.13.3.134	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
5.22.135.239	147.237.77.243	Israel	mobile.idf.il	GPL SCAN myscan	2
91.206.201.94	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
66.249.78.165	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
176.13.0.207	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	1

01-19-2016 to 01-20-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3590
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	900
176.31.117.76	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	688
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	539
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	426
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	318
109.65.189.163	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	273
107.167.98.123	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	255
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	drop		drop	251
46.19.85.47	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	192
5.22.135.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	163
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	143
84.108.44.125	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	142
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	125
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	121
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	120
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	120
158.169.150.9	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	104
158.169.40.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	102
132.3.49.78	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	97
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	93
168.235.196.13	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	93
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	92
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	89
46.116.127.50	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	82
37.26.146.220	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	73
109.67.51.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
31.168.203.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	60
77.126.96.187	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
2.54.49.67	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
185.3.144.112	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
2.54.254.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
46.19.85.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
188.161.7.219	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	48
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	47
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	45
79.178.170.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
46.19.85.169	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
109.107.252.101	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	43
81.218.197.49	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.86.41	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
80.246.130.48	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
77.127.219.238	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
94.159.141.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
85.130.139.95	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	511
80.246.133.192	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	426
2.54.140.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	324
176.13.11.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	271
176.13.11.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	247
109.253.215.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	231
37.46.39.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	216
80.246.136.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	199
79.177.53.57	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.53.57	Block	195
2.54.25.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	191
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	185
176.13.4.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	184
109.253.215.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	178
80.179.141.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	177
46.116.100.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	166
2.54.140.182	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.140.182	Block	146
84.228.141.201	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.141.201	Block	124
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.215.242	Block	124
80.179.141.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	121
80.246.136.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
2.54.177.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
2.54.29.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	114
2.52.61.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
2.54.140.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
2.54.181.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
2.54.29.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
2.54.25.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
212.76.102.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
37.142.64.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
37.46.39.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
37.142.64.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	104
80.246.136.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
185.3.147.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
79.182.62.136	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.62.136	Block	83
2.52.61.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	82
109.253.136.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
46.116.100.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	80
2.54.25.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	78
185.32.179.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
132.70.66.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
176.13.22.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
2.54.161.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
109.253.136.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
176.13.6.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
2.54.181.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	64
212.76.102.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	62