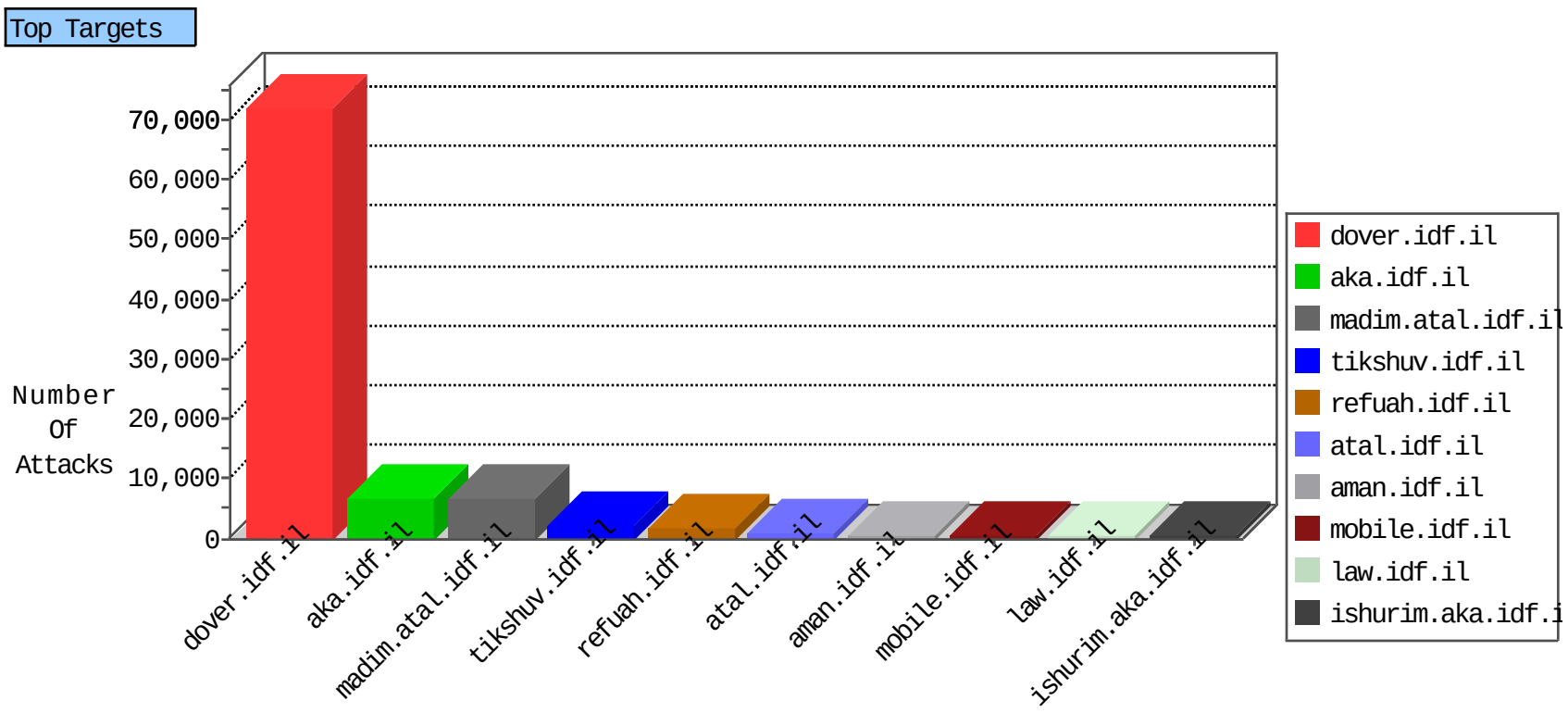
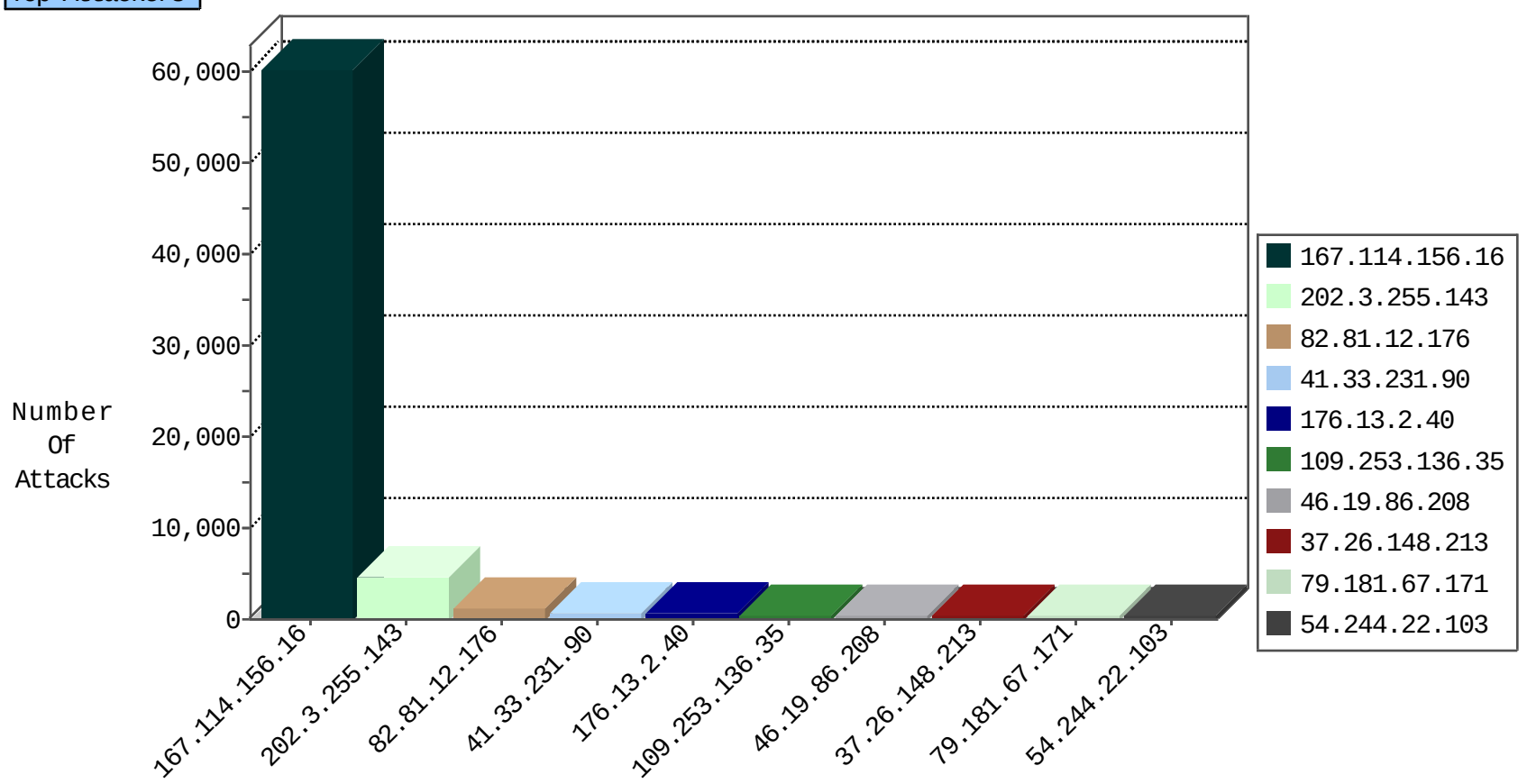
01-20-2016 to 01-21-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-20-2016 to 01-21-2016

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	89489
64.233.172.155	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	7698
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3744
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1195
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	453
37.8.25.138	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	436
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	122
86.132.172.184	United Kingdom	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	93
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	77
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	40
79.182.173.196	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
82.80.136.93	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	12
37.26.146.225	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
66.249.93.107	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	8
82.145.218.194	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
109.66.117.127	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
162.243.3.218	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.109.229.151	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
2.54.138.73	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
190.202.116.34	Venezuela	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	5
122.53.166.142	Philippines	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
112.120.152.8	Hong Kong	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	4
84.228.177.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.165.186	Israel	147.237.72.166	aka.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
84.111.225.26	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
145.225.60.5	Germany	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.182.39.164	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
194.89.24.49	Finland	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
14.99.58.94	India	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
219.250.228.44	Korea, Republic of	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	3
84.108.85.95	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.182.186.220	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.67.168.125	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
207.46.13.49	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.67.201.245	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
222.163.195.35	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
145.225.60.5	Germany	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
207.46.13.193	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
175.136.191.119	Malaysia	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2

01-20-2016 to 01-21-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
203.236.50.22	Korea, Republic of	147.237.77.216	dover.idf.il	C014: HTTP: Fuck in url	Block	24
5.29.53.139	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	12
69.30.218.166	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	10
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	9
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	8
185.120.125.12		147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	8
140.101.20.1	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	5
69.30.218.166	United States	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	5
185.63.188.120	Russian Federation	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	4
87.223.18.84	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	4
157.55.39.156	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	3
69.30.214.38	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
46.120.204.172	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
109.65.121.198	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
91.215.79.231	Russian Federation	147.237.72.166	aka.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	2
158.69.209.141	United States	147.237.77.74	law.idf.il	C106: HTTP: majestic bot	Block	2
2.54.141.221	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.185	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
185.63.188.120	Russian Federation	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	2
91.121.112.142	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
109.65.165.184	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
158.69.209.141	United States	147.237.77.170	maarachot.idf.il	C106: HTTP: majestic bot	Block	2
149.202.48.207	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
91.121.169.194	France	147.237.0.34	tikshuv.idf.il	C106: HTTP: majestic bot	Block	2
69.30.218.166	United States	147.237.77.176	matpash.idf.il	C106: HTTP: majestic bot	Block	2
136.243.103.157	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
158.69.209.141	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
87.223.18.84	Spain	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
158.69.209.141	United States	147.237.76.31	nakchal.idf.il	C106: HTTP: majestic bot	Block	2
46.252.131.34	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
176.13.20.105	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
91.121.169.194	France	147.237.77.74	law.idf.il	C106: HTTP: majestic bot	Block	2
158.69.209.141	United States	147.237.76.86	navy.idf.il	C106: HTTP: majestic bot	Block	2
199.30.24.91	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
88.229.145.165	Turkey	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
151.80.31.120	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.176	France	147.237.0.15	kosher-kravi.idf.i	C228: HTTP: AhrefBot crawler	Block	1
87.69.161.149	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.39.60.178	China	147.237.8.45	e.eitan.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
157.55.39.149	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
46.120.204.172	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
93.63.188.181	Italy	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.188	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
87.106.184.160	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
62.217.146.241	Azerbaijan	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
106.39.60.178	China	147.237.8.46	e.chinuch.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
185.73.39.108		147.237.0.34	tikshuv.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

01-20-2016 to 01-21-2016

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	4391
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	69
95.86.123.137	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	68
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	36
46.19.86.216	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
66.249.78.111	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
37.26.146.166	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	5
168.62.238.153	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	3
93.63.188.181	147.237.77.216	Italy	dover.idf.il	SQL Injection - Select From	3
37.187.24.36	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	3
163.172.13.173	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	3
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	3
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
87.106.184.160	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	3
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	3
95.86.70.197	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
192.198.151.43	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	2
163.172.13.173	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	2
82.102.199.21	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.149.161.186	147.237.8.14	China	e.orchot.idf.il	GPL SCAN nmap TCP	2
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.191	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
41.13.136.157	147.237.77.216	South Africa	dover.idf.il	ET SCAN NMAP -sA (2)	2
182.162.73.59	147.237.0.15	Korea, Republic of	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	2
124.65.196.195	147.237.72.156	China	aman.idf.il	GPL SCAN nmap TCP	2
93.174.93.181	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.117.233.201	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.216	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
176.13.3.134	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
106.120.201.115	147.237.72.156	China	aman.idf.il	GPL SCAN nmap TCP	2
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
143.208.27.192	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.228.207.18	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.28	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
213.8.204.1	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	2
66.249.65.241	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.222	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
121.201.27.61	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.171	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
95.86.124.198	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.81.133	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.3.134	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2

01-20-2016 to 01-21-2016

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	762
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	343
79.177.209.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	268
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	252
132.64.154.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	204
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	201
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	189
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	183
79.180.26.116	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	129
109.253.140.35	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	126
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	123
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	118
148.251.130.181	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	117
148.251.130.181	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	117
145.225.60.5	Germany	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	103
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	94
46.165.208.196	Germany	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	71
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	69
192.116.165.51	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	67
84.94.221.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	57
147.236.138.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	52
212.150.214.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
85.130.173.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
109.253.137.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
41.13.74.30	South Africa	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
85.130.173.177	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	43
216.185.58.177	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	43
221.202.205.222	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	43
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
109.66.187.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
175.18.112.202	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	41
2.54.61.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
95.27.37.160	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.206	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.181.202.151	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
90.174.2.13	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
79.183.103.200	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
172.56.38.6	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	33
46.19.85.117	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
2.52.176.51	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
205.204.17.210	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
94.230.86.244	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.67.171	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	423
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	331
109.253.136.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	307
176.13.2.40	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.2.40	Block	287
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.208	Block	272
37.26.146.166	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.166	Block	207
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	176
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	169
176.13.2.40	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.2.40	Block	163
46.19.86.47	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	163
5.29.131.168	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.131.168	Block	161
185.32.179.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
176.13.18.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
109.253.158.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	136
176.13.2.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
37.26.148.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
37.26.146.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
37.26.148.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	118
109.253.136.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
2.54.152.163	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.152.163	Block	113
109.65.133.152	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.65.133.152	Block	111
85.64.155.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.152.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
2.54.143.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
109.253.136.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	94
176.13.3.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	89
37.142.64.129	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	85
2.54.143.106	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.143.106	Block	84
2.54.133.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.208	Block	79
85.64.155.30	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.64.155.30	Block	79
176.13.18.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	77
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
84.108.26.250	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
185.32.179.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	68
176.228.15.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
37.26.148.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
109.253.150.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
149.78.120.205	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
2.54.160.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
46.121.60.121	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
77.126.82.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
109.253.158.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
2.54.25.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50