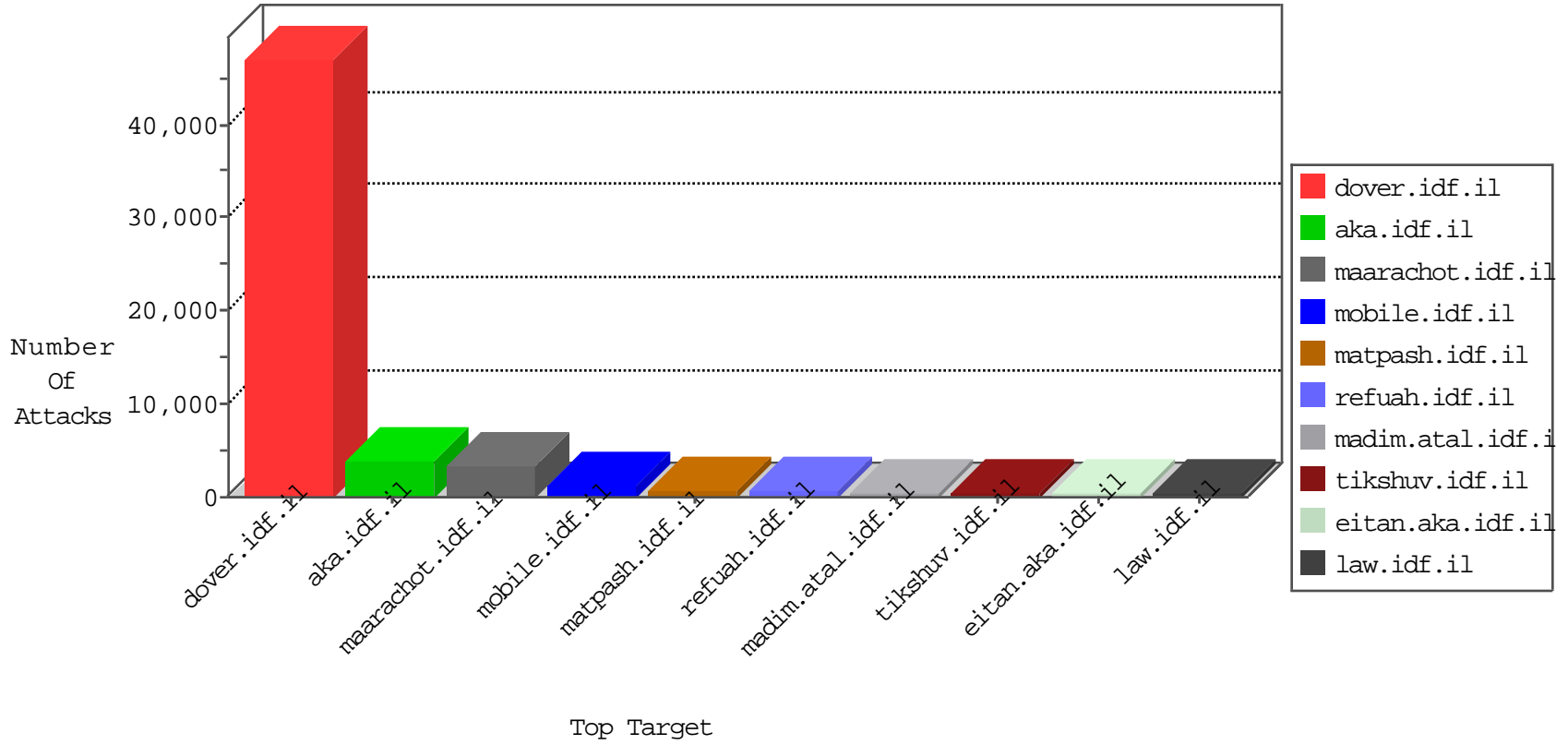


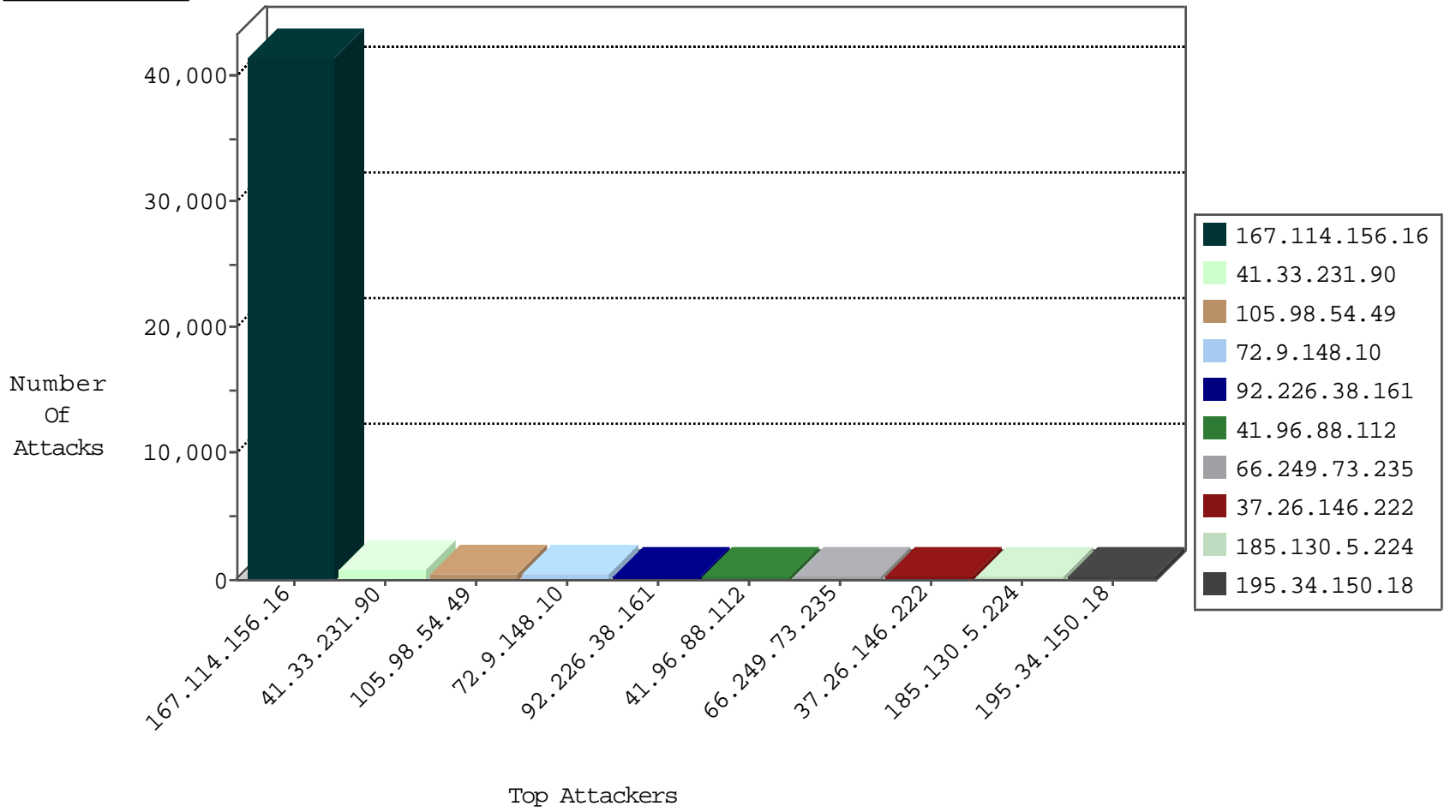
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	89708
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12024
105.98.54.49	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4131
185.99.47.71		147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2970
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1719
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1315
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1134
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	680
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	190
204.93.154.200	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	180
84.228.220.53	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	69
84.228.220.53	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	18
210.123.116.12	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
79.182.181.213	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
41.194.80.146	Satellite Provider	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.108.209.133	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.178.139.52	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.182.181.213	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
8.37.71.39	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.177.15.236	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
8.37.71.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.176.174.180	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
151.0.151.137	Romania	147.237.72.14	dover.idf.il(old)	I4 Source or Dest Port Zero	drop	4
84.109.13.208	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
52.33.66.29	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
67.11.198.109	United States	147.237.76.200	eitan.aka.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
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
8.37.237.212	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
42.200.37.18	Hong Kong	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
197.135.127.194	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
121.201.19.146	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
23.27.220.126	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
70.39.185.210	Satellite Provider	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
123.151.149.222	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.132	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
74.91.124.204	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
192.99.131.107	Canada	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
123.195.116.221	Taiwan	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
106.75.199.192	China	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
195.154.214.162	France	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
68.42.48.136	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
121.3.83.96	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	26
185.120.126.4		147.237.72.166	aka.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	18
41.96.88.112	Algeria	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	12
5.22.130.79	Israel	147.237.0.34	tikshuv.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	3
185.130.5.224		147.237.77.205	prisha.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	3
185.130.5.224		147.237.76.30	himush.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	3
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	3
185.130.5.224		147.237.77.216	dover.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	3
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
66.240.213.93	United States	147.237.76.38	e.e.meitav.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	2
185.130.5.224		147.237.76.42	refuah.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
5.22.130.79	Israel	147.237.72.166	aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	2
185.130.5.224		147.237.77.74	law.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
185.130.5.224		147.237.76.86	navy.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
41.96.88.112	Algeria	147.237.77.216	dover.idf.il	C023: HTTP: administrator in URI	Permit	2
185.130.5.224		147.237.77.235	sviva.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
185.130.5.224		147.237.76.31	nakchal.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
185.130.5.224		147.237.76.200	eitan.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	2
185.130.5.224		147.237.0.19	madim.atal.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
51.254.141.216	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.130.5.224		147.237.77.226	www.chamatz.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
198.20.69.74	United States	147.237.77.212	e.dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.130.5.224		147.237.77.19	law-forum.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.0.34	tikshuv.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
121.200.54.195	India	147.237.77.74	law.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.130.5.224		147.237.77.233	atal.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1
69.30.203.166	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.130.5.224		147.237.72.156	aman.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.130.5.224		147.237.77.234	halag.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
104.45.132.180	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
62.210.107.201	France	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
185.130.5.224		147.237.0.15	kosher-kravi.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
105.103.145.209	Algeria	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
151.80.44.115	Italy	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.8.14	e.orchot.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
62.212.73.211	Netherlands	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.235	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	255
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	92
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	40
41.96.88.112	147.237.77.216	Algeria	dover.idf.il	Admin login page scan - Haviij	34
80.246.130.9	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
77.254.26.127	147.237.77.176	Poland	matpash.idf.il	SERVER-WEBAPP yabb access	6
77.254.26.127	147.237.77.74	Poland	law.idf.il	SERVER-WEBAPP yabb access	6
41.96.88.112	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP admin.php access	6
41.96.88.112	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP adminlogin access	5
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
105.98.54.49	147.237.77.216	Algeria	dover.idf.il	ET SCAN NMAP -sS window 1024	4
41.96.88.112	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP login.htm access	4
5.22.130.79	147.237.0.34	Israel	tikshuv.idf.il	WEB-FRONTPAGE /_vti_bin/ access	3
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
185.130.5.224	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 1024	2
5.22.130.79	147.237.72.166	Israel	aka.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
61.149.161.186	147.237.8.45	China	e.eitan.idf.il	GPL SCAN nmap TCP	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
5.9.96.111	147.237.77.216	Germany	dover.idf.il	Tehila - Perl LWP with fake user agent	2
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	2
183.60.48.25	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
209.126.116.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.69.142	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
176.13.0.159	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
104.199.129.163	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP osCommerce categories.php Arbitrary File Upload And Code Execution	2
66.249.66.53	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
109.253.199.247	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
185.120.126.14	147.237.77.216		dover.idf.il	ET SCAN NMAP -sA (2)	2
41.251.161.255	147.237.76.176	Morocco	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
106.120.201.115	147.237.76.196	China	e.sviva.idf.il	GPL SCAN nmap TCP	2
66.249.81.212	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
176.49.152.157	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
104.143.14.247	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
176.49.152.157	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	2
223.72.232.242	147.237.76.196	China	e.sviva.idf.il	GPL SCAN nmap TCP	2
66.249.78.173	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	2
209.126.116.147	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.254	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
2.54.189.242	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
168.62.238.153	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	2
124.65.196.195	147.237.76.196	China	e.sviva.idf.il	GPL SCAN nmap TCP	2
31.168.89.205	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.63	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2

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	734
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	304
92.226.38.161	Germany	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	268
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	241
89.139.189.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	177
37.26.146.222	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	156
109.64.149.185	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	127
79.177.0.133	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
78.52.159.123	Germany	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	121
109.66.172.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	93
79.179.56.51	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	91
132.64.30.88	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	85
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	77
8.37.237.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	77
70.39.185.210	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	75
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
70.39.185.210	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
46.19.85.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
84.111.138.75	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
109.65.14.227	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
174.64.97.238	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
85.203.17.178	Netherlands	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	50
46.19.86.2	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	49
213.8.122.38	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
5.28.166.15	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
84.228.46.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.85.161	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
207.241.226.221	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	40
5.102.254.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
185.120.126.115		147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	38
79.182.131.130	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
79.183.168.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.183.56.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
37.26.146.222	Israel	147.237.8.45	e.eitan.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
82.80.58.184	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
85.64.162.181	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
84.228.230.135	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
79.179.55.63	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
217.132.23.73	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
79.181.163.55	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
79.176.118.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	32
84.111.23.157	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.96.88.112	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.96.88.112	Block	123
89.139.131.205	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	72
80.246.136.188	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	64
41.96.88.112	Algeria	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.96.88.112	Block	52
109.64.48.184	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.48.184	Block	51
41.96.88.112	Algeria	147.237.77.216	dover.idf.il	PHP Attempt	Block	50
77.254.26.127	Poland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 77.254.26.127	Block	36
82.81.57.208	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	31
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	30
79.177.1.244	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.1.244	Block	20
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	19
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	19
77.254.26.127	Poland	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	18
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	17
37.26.148.182	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 37.26.148.182	Block	17
77.254.26.127	Poland	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 77.254.26.127	Block	16
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	15
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.64.0.157	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.0.157	Block	15
77.254.26.127	Poland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	14
85.250.196.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	12
79.178.209.214	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	12
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	12
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	12
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	11
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	10
37.26.149.240	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	10
5.102.254.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	10
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	9
2.54.48.169	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.54.48.169	Block	8
80.246.136.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
84.108.45.207	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.108.45.207	Block	8
2.52.169.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
77.254.26.127	Poland	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	7
79.176.5.172	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.5.172	Block	7
37.142.200.162	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	7
109.253.214.43	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.214.43	None	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	6
149.78.52.11	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	6
95.86.127.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.205.221	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	6
95.86.123.44	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 95.86.123.44	Block	5
84.108.45.207	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5