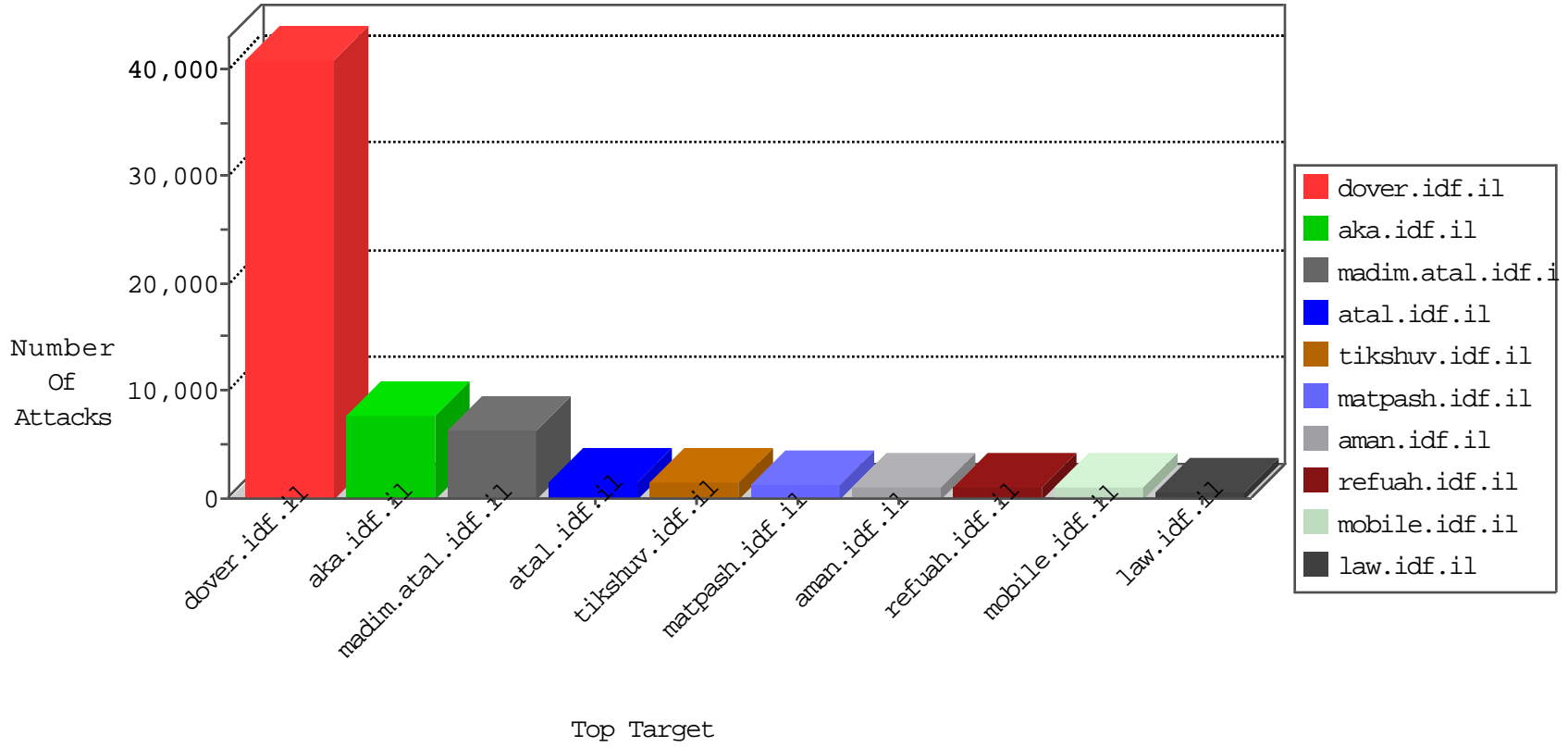


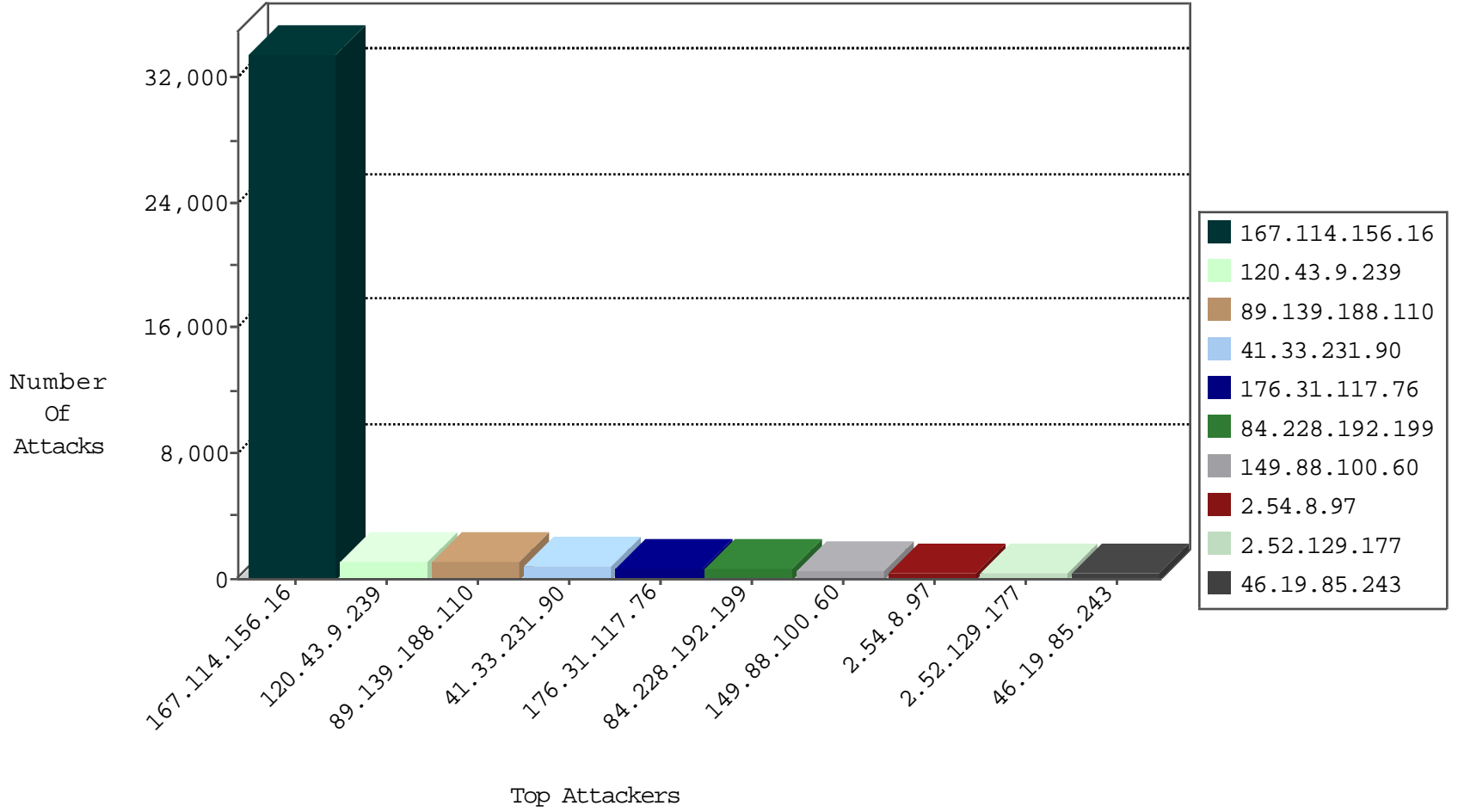
IDF Under Attack Daily Report



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	79356
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	5612
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4437
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2959
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	177
41.107.71.252	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	148
149.88.251.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	53
66.249.73.238	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	36
37.26.146.224	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	28
85.250.89.211	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	27
79.178.139.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
63.141.217.60	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
109.66.55.209	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	12
213.55.105.220	Ethiopia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
41.107.71.252	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8
107.170.91.224	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.110.210.85	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
141.211.173.25	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	5
46.19.85.63	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
5.22.129.234	Israel	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-RST	drop	5
109.66.158.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.180.213.162	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
153.205.78.206	Japan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	4
115.239.228.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	4
149.88.219.246	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	3
115.239.228.10	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	3
221.118.30.101	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
41.190.12.209	Nigeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.179.11.243	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
213.57.215.231	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.il	network flood IPv4 TCP-RST	drop	3
220.181.108.77	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
194.177.16.3	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
213.57.215.231	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.43.9.239	China	147.237.77.226	www.chamatz.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	33
120.43.9.239	China	147.237.72.156	aman.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.76.200	eitan.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.0.34	tikshuv.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	31
120.43.9.239	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	29
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
178.137.18.190	Ukraine	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	15
120.43.9.239	China	147.237.76.200	eitan.aka.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.72.166	aka.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.77.226	www.chamatz.aka.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.76.86	navy.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.77.233	atal.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.0.34	tikshuv.idf.il	0854: HTTP: upload* Access	Block	9
120.43.9.239	China	147.237.72.156	aman.idf.il	0854: HTTP: upload* Access	Block	9
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	0854: HTTP: upload* Access	Block	8
120.43.9.239	China	147.237.77.176	matpash.idf.il	0854: HTTP: upload* Access	Block	8
120.43.9.239	China	147.237.77.74	law.idf.il	0854: HTTP: upload* Access	Block	7
37.59.40.198	France	147.237.72.166	aka.idf.il	12651: HTTP: Open Flash Chart PHP File Upload Vulnerability	Block	6
46.19.86.60	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
72.9.157.128	United States	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	2
104.45.132.180	United States	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
185.130.5.207		147.237.76.147	chinuch.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
198.20.69.74	United States	147.237.76.202	e.halag.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
172.245.224.226	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
69.30.205.218	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
23.94.153.178	United States	147.237.76.200	eitan.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
104.45.132.180	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
185.130.5.207		147.237.76.147	chinuch.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
51.255.48.155	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
209.58.178.49	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
69.30.213.82	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
23.94.153.178	United States	147.237.76.200	eitan.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.200	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
136.243.5.215	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.130.5.207		147.237.76.30	himush.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
23.94.153.178	United States	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.120.173.82	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
192.187.121.66	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
136.243.103.92	Germany	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
23.94.153.178	United States	147.237.76.42	refuah.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
104.45.132.180	United States	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
185.130.5.207		147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1

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	92
64.233.173.161	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	80
84.228.80.92	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	6
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
168.63.206.180	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
168.63.206.180	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
168.63.206.180	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
168.63.206.180	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
168.63.206.180	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.67.115.69	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	4
168.63.206.180	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
80.246.133.87	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
31.43.20.43	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sA (2)	4
168.63.206.180	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
173.199.74.136	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.234	United States	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.111.182.98	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	3
173.199.74.136	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
173.199.74.136	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
173.199.74.136	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential VNC Scan 5900-5920	3
168.63.206.180	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.81.199	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
168.63.206.180	147.237.76.177	United States	noore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
173.199.74.136	147.237.76.176	United Kingdom	test.noore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
176.50.139.113	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
173.199.74.136	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
173.199.74.136	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
168.62.238.153	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
109.111.182.98	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	2
173.199.74.136	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
168.63.206.180	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
173.199.74.136	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.73.206	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
84.108.38.77	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.182	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
168.63.206.180	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
109.111.182.98	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.188.110	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	846
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	789
176.31.117.76	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	727
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	268
212.150.218.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	268
79.179.105.15	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	237
87.68.166.126	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	196
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
95.90.251.171	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	123
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	103
89.139.188.110	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	97
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	95
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	94
89.139.188.110	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	92
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
77.125.3.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
84.229.245.21	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
79.176.32.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
84.229.29.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	65
172.56.2.199	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	64
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	63
104.236.203.68		147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
79.181.106.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
176.13.1.79	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
104.236.203.68		147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	52
2.52.49.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	52
91.64.54.129	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	52
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
79.180.133.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.57.190.230	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	45
109.66.56.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	45
46.57.190.230	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	45
80.246.133.109	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
176.228.154.105	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
46.19.85.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
37.142.135.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
176.13.10.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
79.182.27.143	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
84.228.144.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.176.63.110	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.182.147.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
213.55.105.220	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
45.35.64.142		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
5.29.183.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.192.199	Block	385
79.178.118.150	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	251
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	244
2.54.8.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	243
2.52.129.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	233
149.88.100.60	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.100.60	Block	222
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 84.228.192.199	Block	174
2.54.29.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	145
2.52.129.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
87.69.125.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	131
2.52.18.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
2.52.18.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.18.137	Block	125
46.117.160.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
109.253.204.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
149.88.100.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
149.88.100.60	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 149.88.100.60	Block	114
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.54.161.219	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	107
176.13.1.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
84.228.192.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.204.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
2.54.8.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
185.32.179.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
2.54.29.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.143.128	Block	91
5.29.105.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
109.253.192.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
2.54.8.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	85
87.69.35.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
109.66.41.205	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.41.205	Block	81
84.109.24.224	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
5.22.129.234	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.129.234	Block	75
2.54.161.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.183	Block	74
185.32.179.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
87.69.125.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
176.228.154.105	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
79.177.145.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
87.69.35.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
176.13.1.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
109.66.107.237	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
2.52.18.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
213.57.240.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
95.35.133.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.121.93.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
109.253.142.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46