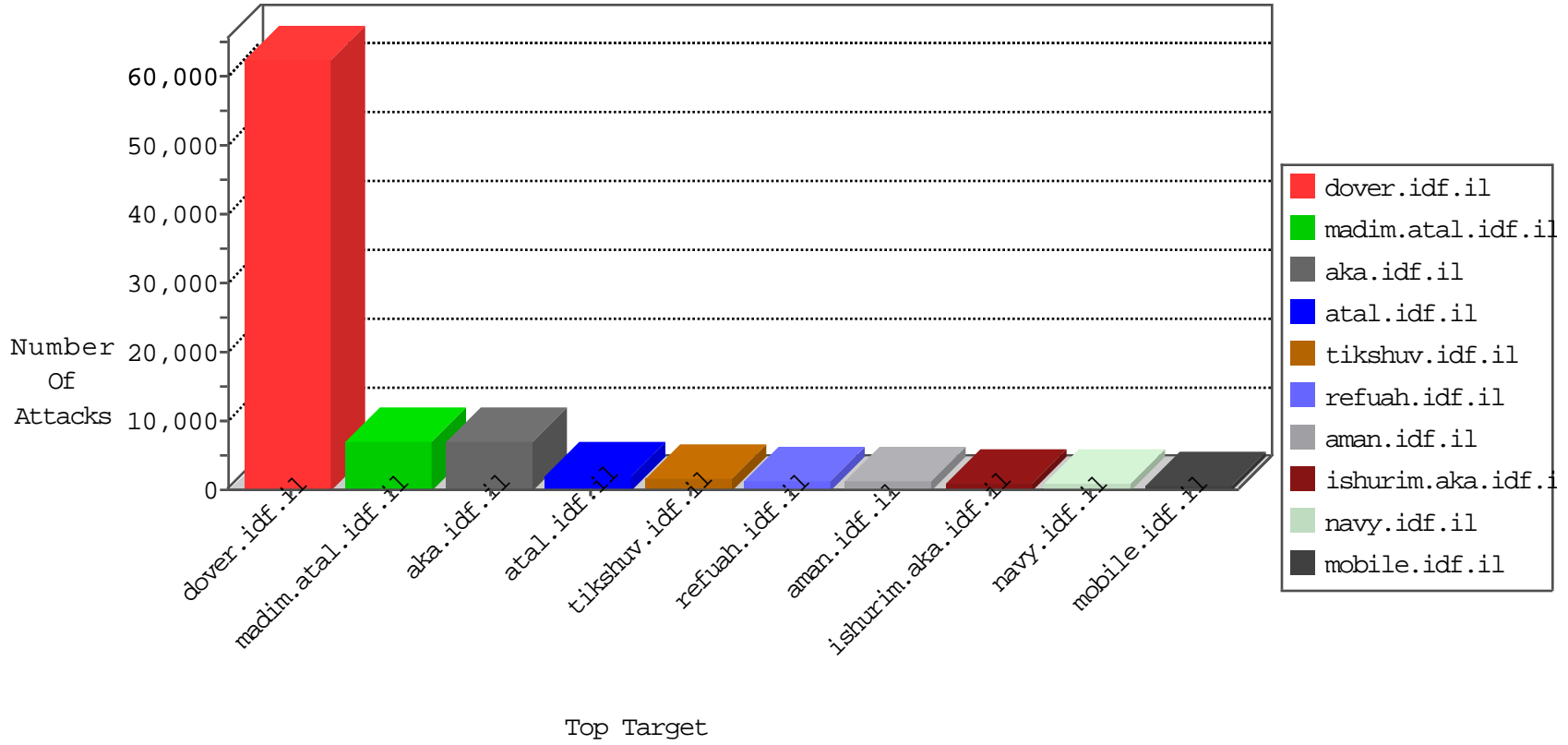


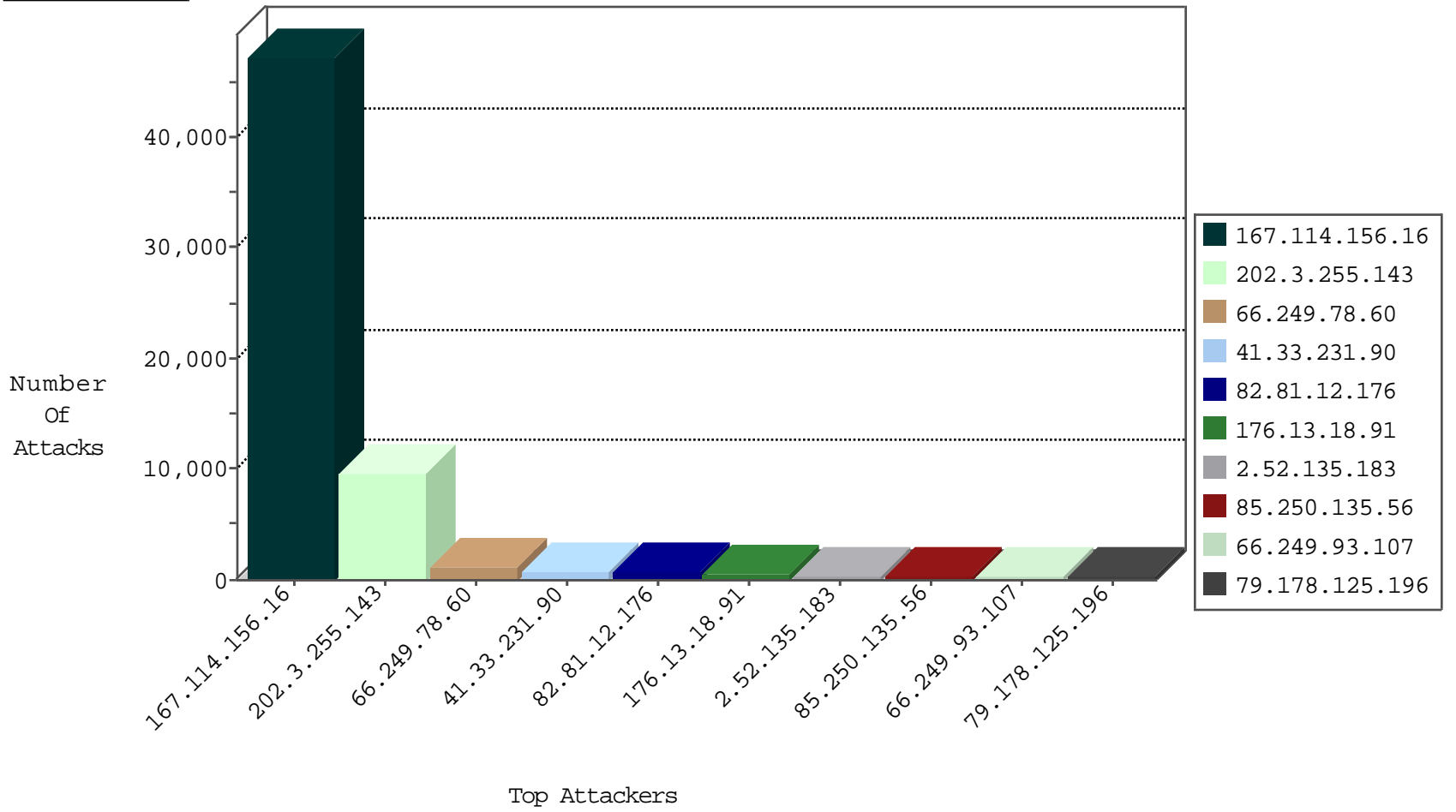
IDF Under Attack Daily Report



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	89767
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8815
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6464
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1209
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	654
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	457
66.249.64.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	292
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
91.197.62.30	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	94
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
91.197.62.30	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Top	drop	44
149.78.4.156	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
81.218.165.186	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	21
193.227.133.100	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
109.253.192.5	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
82.132.220.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
31.168.232.150	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	12
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
185.93.35.18		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
37.26.146.231	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
109.66.99.58	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
66.249.64.92	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
194.90.37.175	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
79.177.11.229	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
173.252.90.102	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
94.4.197.178	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
81.218.165.186	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.178.168.149	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
69.31.51.40	Anonymous Proxy	147.237.0.34	tikshuv.idf.il	Frk_Purple_Con_Limit_Http	drop	3
81.218.206.82	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
79.180.152.75	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.246.140.176	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	3
77.153.148.47	France	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.109.181.187	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
123.151.149.222	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
8.37.231.92	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
113.197.51.199	Pakistan	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
69.31.51.40	Anonymous Proxy	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
113.64.47.110	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.126.211	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	30
212.199.224.24	Israel	147.237.77.74	law.idf.il	C157: HTTP: Access to GetFile.aspx	Block	24
109.226.45.219	Israel	147.237.0.34	tikshuv.idf.il	C208: HTTP: Range in the Header	Block	15
213.8.204.70	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	13
85.250.135.24	Israel	147.237.77.170	maarachot.idf.il	C208: HTTP: Range in the Header	Block	12
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	12
185.130.5.247		147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
40.113.8.22	United States	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
40.113.8.22	United States	147.237.0.34	tikshuv.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
62.90.147.145	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	8
192.117.9.26	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
180.245.57.195	Indonesia	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	8
79.182.17.38	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
37.26.147.179	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
84.111.70.5	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	7
109.66.55.229	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
132.74.58.146	Israel	147.237.77.170	maarachot.idf.il	C208: HTTP: Range in the Header	Block	6
79.181.235.48	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
109.67.52.220	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
37.26.146.234	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
109.64.204.145	Israel	147.237.76.30	himush.idf.il	C208: HTTP: Range in the Header	Block	6
62.0.54.2	Israel	147.237.76.31	nakchal.idf.il	C004: HTTP: options method (Microsoft)	Block	6
185.130.5.247		147.237.76.42	refuah.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
40.113.8.22	United States	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.130.5.235		147.237.76.42	refuah.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
84.108.37.223	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	5
185.130.5.235		147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.130.5.247		147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.130.5.247		147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
79.182.216.163	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	5
185.130.5.235		147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
77.127.177.251	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
85.250.170.7	Israel	147.237.0.34	tikshuv.idf.il	C208: HTTP: Range in the Header	Block	4
10.0.0.2		147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
10.0.0.3		147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
212.179.79.250	Israel	147.237.77.170	maarachot.idf.il	C208: HTTP: Range in the Header	Block	3
93.172.131.51	Israel	147.237.0.34	tikshuv.idf.il	C208: HTTP: Range in the Header	Block	3
197.38.205.20	Egypt	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	3
31.13.112.118	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	3
31.13.112.122	Ireland	147.237.76.86	navy.idf.il	C208: HTTP: Range in the Header	Block	2
79.183.50.175	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
185.130.5.235		147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
84.108.5.155	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
40.113.8.22	United States	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
79.181.181.170	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
5.29.233.119	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
80.179.13.58	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
46.38.63.9	Russian Federation	147.237.77.216	dover.idf.il	C208: HTTP: Range in the Header	Block	2
40.113.8.22	United States	147.237.0.34	tikshuv.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2

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	8785
66.249.78.60	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1203
66.249.93.107	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	371
177.185.194.92	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	93
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	66
213.204.101.24	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	26
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	6
64.251.25.176	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
66.96.128.60	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	5
66.249.66.81	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	4
200.59.205.238	147.237.77.74	Argentina	law.idf.il	SQL Injection - Select From	4
195.140.210.83	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	3
216.249.107.200	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
184.173.233.226	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	3
80.246.130.207	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	3
212.199.57.205	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	3
66.249.78.79	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	3
77.126.166.33	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	3
23.91.70.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
82.165.24.123	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	3
66.249.64.17	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
184.106.114.136	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
109.65.130.19	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
40.113.8.22	147.237.0.15	United States	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.247	147.237.0.17		m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
66.249.75.37	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.136.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
184.168.193.34	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
213.41.36.16	147.237.77.216	United Kingdom	dover.idf.il	GPL SCAN nmap TCP	2
192.198.151.45	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	2
40.113.8.22	147.237.0.34	United States	tikshuv.idf.il	ET WEB_SERVER Muieblackcat scanner	2
109.65.130.19	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
168.62.238.153	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
50.97.146.246	147.237.72.156	United States	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.130.5.235	147.237.0.15		kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
117.79.130.206	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.12.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
105.224.209.46	147.237.77.216	South Africa	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.59.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	901
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	815
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	460
79.179.177.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	270
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	214
69.31.51.40	Anonymous Proxy	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	152
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	141
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	117
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	97
217.132.4.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
8.37.231.92	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	90
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
176.122.88.16	Ukraine	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	66
5.22.135.140	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
151.80.108.176	Italy	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
151.80.108.176	Italy	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
46.19.86.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
5.102.253.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
2.54.153.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	52
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	52
46.19.85.50	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
82.80.23.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
2.54.44.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
193.227.133.100	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
213.8.204.64	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	47
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	46
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	46
2.54.183.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
2.54.36.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	45
103.242.166.254	Papua New Guinea	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
62.90.140.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
207.241.229.192	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	39
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
80.246.137.27	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
2.52.24.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.5.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
94.159.149.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
46.19.86.153	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	34
84.108.99.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
46.19.85.202	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
217.132.110.23	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	32
141.0.14.74	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	32
213.8.204.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
213.8.204.45	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	31
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
31.154.154.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
79.182.20.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
79.180.136.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	277
2.52.135.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	217
213.151.36.44	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
85.250.135.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	189
79.178.125.196	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.178.125.196	Block	171
109.253.135.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
109.66.55.229	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
185.32.179.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	165
176.13.18.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	160
80.246.137.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	156
46.19.86.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
2.54.158.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	139
2.52.135.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	139
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
149.78.247.105	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	133
84.229.30.89	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	132
46.19.86.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
109.253.214.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
109.253.135.225	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.135.225	Block	118
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
46.19.85.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
2.52.52.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
2.54.158.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
79.178.125.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.13.18.91	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.18.91	Block	106
85.250.135.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
176.13.4.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
31.168.64.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
109.253.213.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
31.210.184.217	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.210.184.217	Block	90
80.179.13.58	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 80.179.13.58	Block	88
85.250.135.56	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 85.250.135.56	Block	86
82.166.12.34	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 82.166.12.34	Block	86
85.250.199.42	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
31.168.64.190	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.168.64.190	Block	84
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
109.65.149.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
2.54.48.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
2.52.25.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
80.246.136.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
79.182.19.53	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
176.13.16.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
213.8.204.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
109.253.199.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	58
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
2.54.142.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
2.52.24.101	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	55