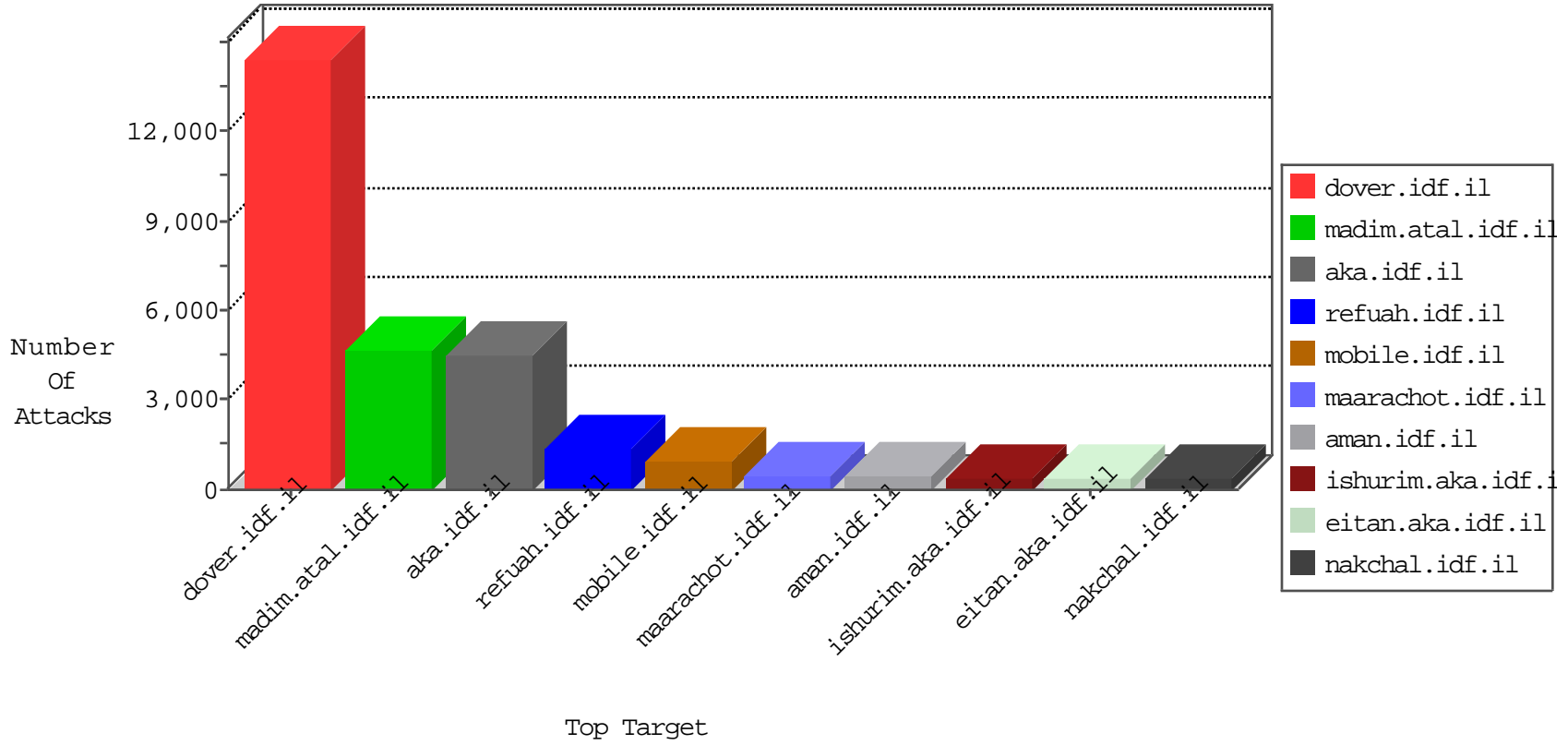


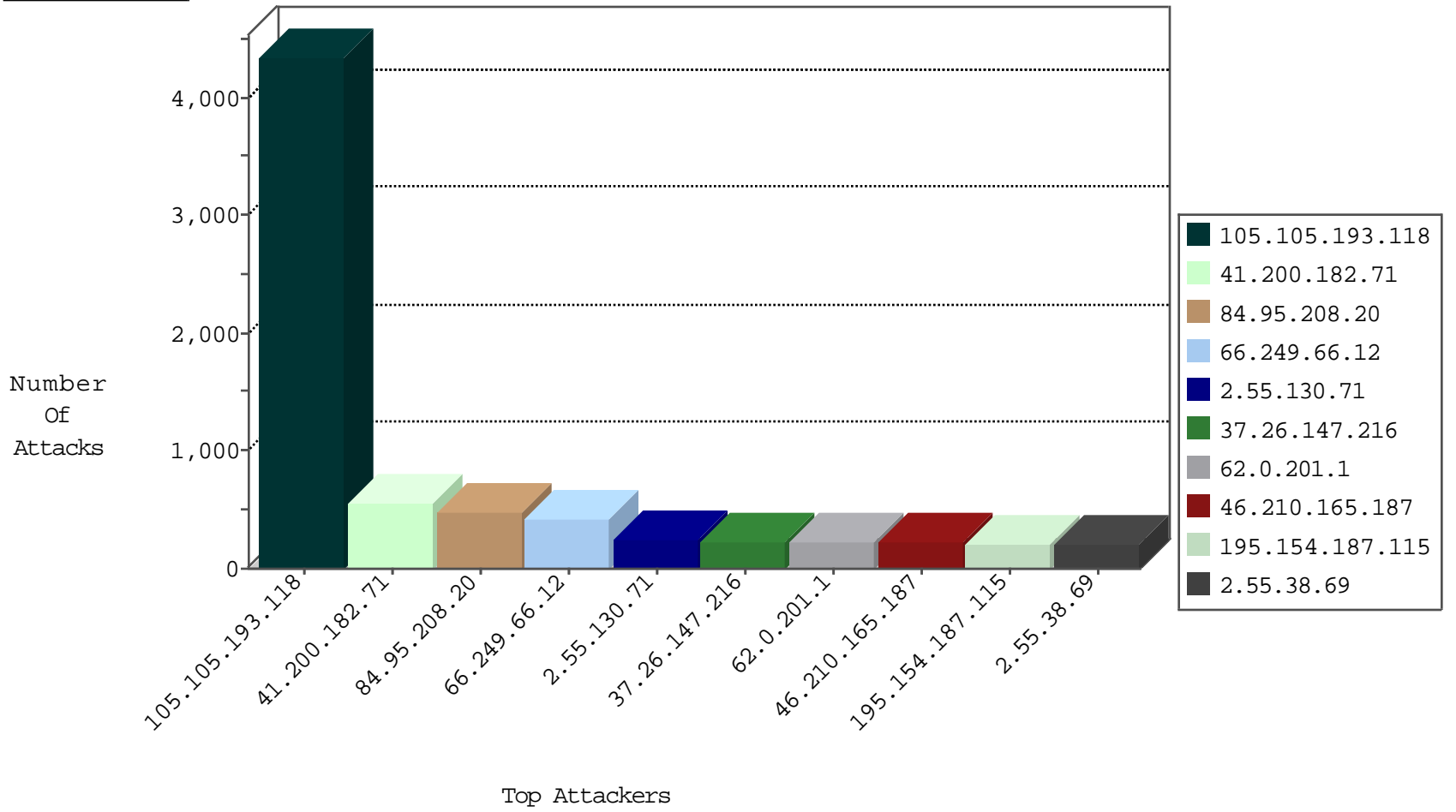
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	9095
105.105.193.118	Algeria	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	9049
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6654
105.105.193.118	Algeria	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3526
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2063
105.105.193.118	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	714
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
109.65.90.105	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	80
91.141.3.52	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	72
37.237.192.39	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	66
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	46
176.13.12.205	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
185.32.179.136	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
185.32.179.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
176.13.233.174	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
80.246.138.145	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
2.55.133.94	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
217.132.33.124	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
77.139.101.27	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
2.53.140.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
66.249.93.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
87.71.35.170	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
79.180.122.72	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.19.86.235	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
79.178.30.171	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
46.120.92.93	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
85.65.33.246	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
87.71.24.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
80.178.189.167	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
5.29.171.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
5.102.195.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
2.55.154.168	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.66.33.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.253.222.62	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
37.142.11.16	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.181.195.175	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
77.127.73.83	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
176.13.5.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
80.246.137.155	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
84.94.208.121	Israel	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	TCP handshake violation, first packet not syn	drop	4
195.228.168.121	Hungary	147.237.76.201	e.atal.idf.il	L4 Source or Dest Port Zero	drop	4
213.8.204.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
85.65.38.117	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
80.246.138.148	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	194
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	61
62.210.90.118	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	36
54.175.139.222	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	20
54.152.103.188	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	20
216.119.112.144	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
85.8.28.214	Sweden	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	13
213.174.55.11	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	12
87.242.112.45	Russian Federation	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
216.119.125.57	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
52.90.55.176	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	10
91.200.12.47	Ukraine	147.237.77.74	law.idf.il	C1000016: HTTP: administrator in URI	Permit	8
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Permit	8
91.209.51.22	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	8
87.242.112.45	Russian Federation	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.112.144	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.154.187.115	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	6
91.219.122.2	Poland	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.57	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.46.74	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.17.96.33	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.229	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
89.44.144.244	Romania	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
91.194.84.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
38.110.11.92	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	4
176.9.131.69	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.32.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
88.198.16.12	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
195.154.187.115	France	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
62.210.90.118	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.254.129.90	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.255.20	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
41.200.182.71	Algeria	147.237.77.216	dover.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	2
195.154.187.115	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.48.155	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.255.20	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.90.118	France	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.187.115	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.48.155	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
85.8.28.214	Sweden	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.90.118	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.90.118	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDF

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	411
216.119.112.144	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	72
216.119.125.57	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	51
87.242.112.45	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	46
213.174.55.11	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	27
91.219.122.2	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	14
50.63.196.229	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	12
87.69.47.220	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	10
38.110.11.92	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
89.44.144.244	147.237.77.74	Romania	law.idf.il	SQL Injection - Select From	8
184.168.46.74	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
187.17.96.33	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	8
62.210.97.57	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
27.97.139.181	147.237.76.200	India	eitan.aka.idf.il	GPL SCAN nmap TCP	4
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
66.249.64.163	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
141.226.162.74	147.237.77.226	Israel	www.chamatz.aka.idf.il	INDICATOR-SCAN myscan	3
46.219.66.30	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
105.105.193.118	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP backup access	3
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	3
141.226.162.74	147.237.77.226	Israel	www.chamatz.aka.idf.il	GPL SCAN myscan	3
46.183.223.228	147.237.8.46	Latvia	e.chimuch.idf.il	ET SCAN Potential SSH Scan	2
95.163.144.203	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
62.0.104.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
54.175.4.38	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
117.21.173.9	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
116.209.196.7	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
79.178.185.157	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
121.32.129.130	147.237.77.216	China	dover.idf.il	GPL SCAN nmap TCP	2
74.69.161.0	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
46.19.86.255	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
185.27.106.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
46.183.223.228	147.237.76.44	Latvia	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.76.106	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.26.147.197	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.69.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
117.21.173.9	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
218.24.171.223	147.237.76.147	China	chinuch.aka.idf.il	GPL SCAN nmap TCP	2
91.121.147.218	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
59.46.193.114	147.237.76.147	China	chinuch.aka.idf.il	GPL SCAN nmap TCP	2
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
124.8.223.198	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
46.183.223.228	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN Potential SSH Scan	2
117.21.173.9	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
2.55.166.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.27.85.27	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential SSH Scan	1
183.106.209.187	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.69.161.0	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Potential SSH Scan	1
106.1.112.199	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.105.193.118	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	581
62.0.201.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	222
8.37.237.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	146
5.102.195.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	143
109.253.197.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
194.90.151.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	94
85.250.86.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	92
109.65.4.134	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	87
223.24.36.2	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
2.53.190.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
109.63.202.15	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
37.236.8.50	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
84.111.38.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	58
95.86.80.164	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.200.182.71	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
185.99.17.218	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
81.218.89.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
84.229.28.9	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
141.226.218.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
8.37.237.141	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
82.132.237.95	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
82.80.48.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
210.4.97.2	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.199.34.114	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	39
37.142.10.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
77.138.218.97	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	36
62.0.242.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
107.167.108.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
176.13.12.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
46.19.85.246	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
77.124.40.159	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
66.249.64.81	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.0.232.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
2.53.58.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.0.207.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
176.13.4.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.65.130.67	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
2.53.175.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
87.105.15.139	Poland	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	29

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.105.193.118	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.105.193.118	Block	1261
41.200.182.71	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.200.182.71	Block	474
2.55.130.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	248
37.26.147.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	228
46.210.165.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	225
2.55.38.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	190
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	139
85.65.232.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
85.64.244.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
109.253.245.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
2.53.136.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
46.19.86.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
176.13.230.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.225.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	104
2.53.157.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
109.253.198.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
80.246.138.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
2.53.51.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
37.26.147.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
85.65.98.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
80.246.138.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
80.246.137.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
87.70.20.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.53.40.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	82
185.32.179.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
37.26.149.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.197.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
2.53.40.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
176.13.6.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.55.20.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.53.32.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
109.253.142.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.53.130.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
84.109.13.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
80.246.136.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
182.232.38.157	Thailand	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
188.120.156.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
80.246.137.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
176.13.230.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.234.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.13.22.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
2.53.11.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.53.135.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31