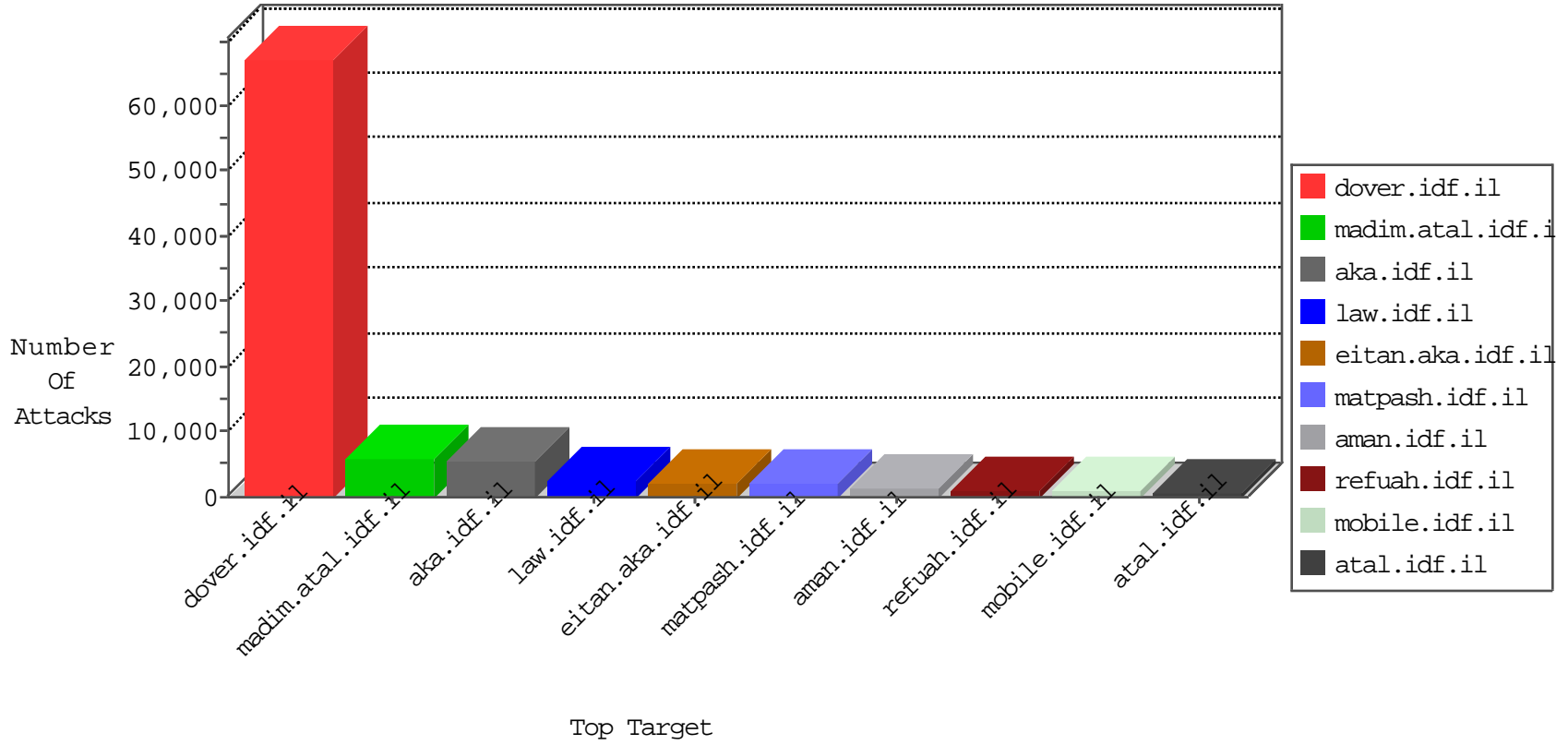


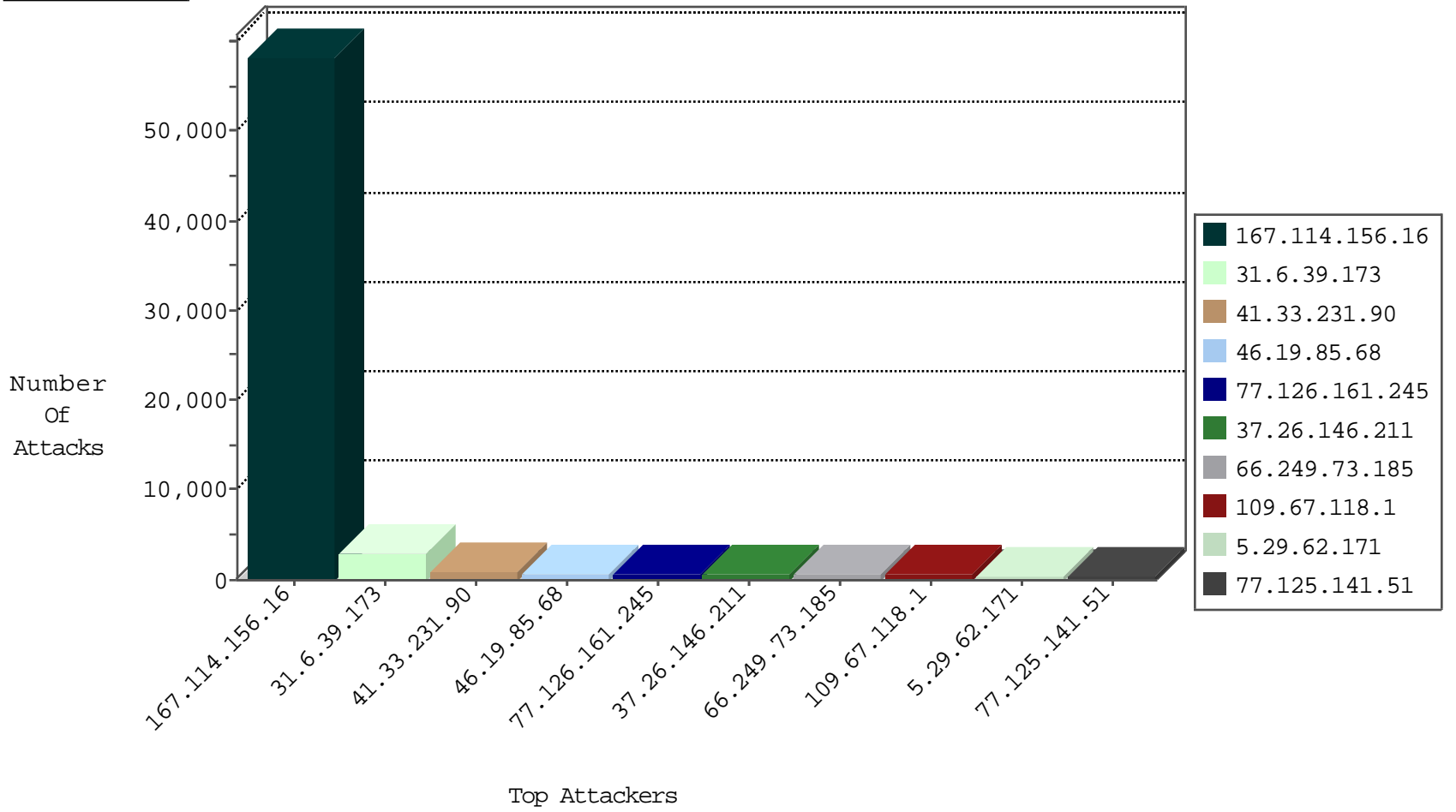
IDF Under Attack Daily Report



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	90389
31.6.39.173	Spain	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	46893
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8056
66.249.66.39	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3742
66.249.64.254	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2905
46.43.110.96	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2378
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1596
54.244.22.103	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	741
66.249.66.65	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	565
220.181.108.110	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	288
66.249.74.97	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	285
204.93.154.203	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	195
66.249.66.1	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	137
8.37.227.139	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
188.49.61.249	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
188.49.61.249	Saudi Arabia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	14
66.249.64.243	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
79.183.14.170	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	7
79.176.205.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
109.66.65.177	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
76.219.164.154	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
66.249.73.185	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.108.82.13	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
91.211.116.32	Ukraine	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
220.181.108.116	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
171.250.102.22	Vietnam	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
188.49.61.249	Saudi Arabia	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
153.31.119.142	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
8.37.224.40	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Https	drop	2
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
58.215.79.100	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
115.231.222.40	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
123.151.42.61	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Udp	drop	2
8.37.227.139	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
69.25.27.116	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.181	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
188.49.61.249	Saudi Arabia	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Https	drop	1
62.209.11.136	Bahrain	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
93.158.203.169	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
84.111.162.137	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
195.140.210.83	Germany	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
91.218.29.20	Ukraine	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
85.64.113.244	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	4
176.228.140.19	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.183.160.142	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
195.154.211.26	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
5.29.145.33	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.188.35	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
94.188.43.181	Russian Federation	147.237.72.166	aka.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	2
195.154.217.38	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.211.30	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.216.122	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
84.228.83.122	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.211.94	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
84.228.165.22	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.165.15.193	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
59.58.107.199	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
195.154.180.69	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.191.208	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
51.254.121.184	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
161.202.41.12	Netherlands	147.237.76.200	eitan.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
161.202.41.12	Netherlands	147.237.0.15	kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
195.154.188.188	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.240	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
88.243.35.221	Turkey	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
199.127.226.150	United States	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1
69.30.239.106	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.211.230	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.191.213	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
161.202.41.12	Netherlands	147.237.76.31	nakchal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
188.165.15.79	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
161.202.41.12	Netherlands	147.237.77.176	matpash.idf.il	C003: HTTP: phpMyAdmin access	Block	1
51.254.141.216	United Kingdom	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
161.202.41.12	Netherlands	147.237.0.19	madim.atal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
195.154.188.224	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
91.121.60.119	France	147.237.0.34	tikshuv.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
167.114.229.247	Canada	147.237.76.177	ncore.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
77.125.99.250	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
24.230.181.31	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.194.47	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
161.202.41.12	Netherlands	147.237.76.42	refuah.idf.il	C003: HTTP: phpMyAdmin access	Block	1
195.154.188.74	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.217.114	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.127	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
161.202.41.12	Netherlands	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	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	94
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	90
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	16
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	14
195.140.210.83	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	10
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.74.97	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
66.249.73.193	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	6
195.154.211.26	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	4
195.154.216.123	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	4
66.249.81.196	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	4
91.218.29.20	147.237.77.176	Ukraine	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
195.154.211.26	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	4
195.154.211.26	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	4
195.154.188.35	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	4
195.154.188.35	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	3
195.154.211.94	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	3
195.154.216.123	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	3
195.154.191.208	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	3
218.104.49.211	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	3
195.154.211.94	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	3
31.6.39.173	147.237.77.216	Spain	dover.idf.il	ET SCAN NMAP -sS window 1024	3
218.104.49.211	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	3
195.154.211.94	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	3
195.154.188.35	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	3
195.154.216.123	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	3
195.154.211.94	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	3
195.154.216.122	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	3
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
40.76.57.67	147.237.0.19	United States	medim.atal.idf.il	ET SCAN Potential SSH Scan	2
195.154.188.74	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
195.154.211.26	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.154.216.165	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.154.211.150	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
31.6.71.154	147.237.76.30	Poland	himush.idf.il	ET SCAN NMAP -sS window 1024	2
61.153.237.122	147.237.76.196	China	e.sviva.idf.il	GPL SCAN nmap TCP	2
195.154.216.164	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
195.154.211.150	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	2
195.154.188.224	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.154.216.164	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
66.249.69.26	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
37.238.75.80	147.237.76.147	Iraq	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
195.154.188.188	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
195.154.188.35	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
66.249.66.65	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.154.194.47	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
195.154.188.186	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
31.184.198.90	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
162.222.185.165	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	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	835
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	521
109.67.118.1	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	465
77.125.141.51	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	423
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	264
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	218
46.166.170.3	Lithuania	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	174
188.49.61.249	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	112
213.57.129.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	98
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.86.148	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
110.85.68.47	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	82
100.100.66.25		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	82
100.100.117.81		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	74
185.3.144.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	68
100.100.61.250		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
149.88.156.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	67
213.57.133.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	63
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
100.100.15.0		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	60
100.100.34.130		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	58
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	57
109.67.41.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
99.232.90.253	Canada	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
84.94.36.185	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
77.126.18.94	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
84.228.119.67	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
100.100.39.250		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	49
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.54.141.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
100.100.15.0		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	47
100.100.0.229		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	47
100.100.23.143		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	47
8.37.224.40	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
100.100.119.229		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	46
100.100.11.84		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	46
213.57.128.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
2.52.184.23	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
79.182.181.144	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.86.11	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
100.100.52.185		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.19.86.80	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
46.43.110.96	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	40
100.100.77.54		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	38

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.161.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	343
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.68	Block	315
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	301
5.29.62.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	267
94.159.215.44	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.215.44	Block	264
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	259
79.181.61.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	203
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.68	Block	182
77.126.99.29	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.126.99.29	Block	175
77.126.161.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
37.26.148.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
109.65.6.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	136
37.26.148.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	135
176.13.21.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	129
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
62.128.41.133	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 62.128.41.133	Block	117
176.13.3.64	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.3.64	Block	114
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
5.29.62.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
176.13.3.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
5.29.62.171	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 5.29.62.171	Block	107
5.29.242.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
77.126.99.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
37.142.210.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
176.13.4.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
176.12.151.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
176.12.151.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	90
87.69.141.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
80.246.136.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
109.65.6.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
5.29.242.139	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.242.139	Block	70
2.54.168.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
176.13.21.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
46.120.248.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
46.19.85.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
176.13.9.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
46.120.69.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
176.13.11.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
46.19.85.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
85.65.111.136	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.111.136	Block	47
87.69.141.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
79.179.150.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
109.67.118.1	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.67.118.1	Block	45
176.12.145.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
77.126.161.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	42
93.173.230.154	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
77.126.99.29	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 77.126.99.29	Block	39