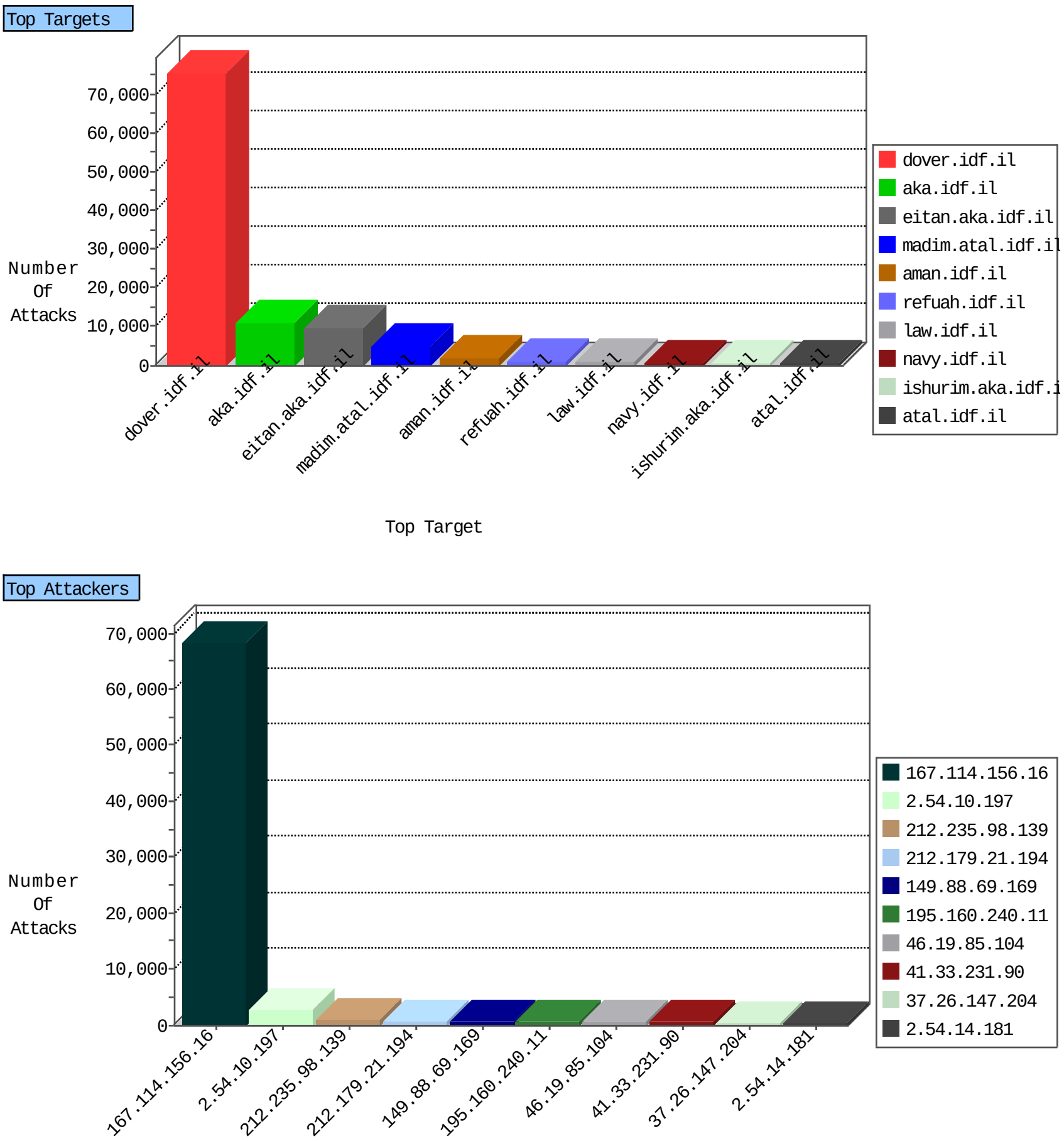
12-01-2015 to 12-02-2015

IDF Under Attack Daily Report



12-01-2015 to 12-02-2015

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	90511
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	40892
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	17269
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4952
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	417
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	208
66.249.64.153	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	187
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	TCP Scan (vertical)	drop	133
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
66.249.64.186	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	97
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
66.249.66.1	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	72
82.145.218.177	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	41
84.109.125.65	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	15
79.178.108.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	11
109.64.107.62	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	9
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
37.26.148.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
80.246.137.222	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	6
219.111.158.124	Japan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	6
84.108.204.65	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
46.19.86.89	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.217.192	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	5
109.64.107.62	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	5
109.64.107.62	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
79.183.4.68	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4
84.109.130.231	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.179.4.105	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
84.108.62.227	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	3
79.182.217.248	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.7	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
198.20.99.130	Netherlands	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
183.60.48.25	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.145.223.56	Europe	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
204.42.253.130	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
93.174.93.151	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
213.57.128.79	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
96.44.187.158	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
93.174.93.146	Netherlands	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
112.198.79.54	Philippines	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
185.56.82.38	Netherlands	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.130	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.8	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2

12-01-2015 to 12-02-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.211.70.193	Netherlands	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
213.179.60.10	United Kingdom	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
95.211.70.193	Netherlands	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
23.91.70.63	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
189.38.90.144	Brazil	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.179.60.10	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
103.21.58.191	India	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
211.23.251.92	Taiwan	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
74.84.136.105	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
63.143.34.37	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
37.58.75.46	Netherlands	147.237.76.147	chinuch.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.58.75.46	Netherlands	147.237.77.235	sviva.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.58.75.46	Netherlands	147.237.77.233	atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.58.75.46	Netherlands	147.237.76.31	nakchal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
37.58.75.46	Netherlands	147.237.77.234	halag.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
59.58.107.199	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
63.143.34.37	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
197.165.237.19	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	3
176.228.161.125	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	3
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	3
185.106.94.2		147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	2
41.96.104.129	Algeria	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	2
195.154.211.20	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
52.1.90.117	United States	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.230	France	147.237.0.34	tikshuv.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
142.4.214.124	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.188.158	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
37.58.75.46	Netherlands	147.237.77.235	sviva.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
161.202.41.12	Netherlands	147.237.76.30	himush.idf.il	C003: HTTP: phpMyAdmin access	Block	1
195.154.216.86	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
37.58.75.46	Netherlands	147.237.77.233	atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.188.186	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
74.84.136.105	United States	147.237.72.166	aka.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	1
185.106.94.2		147.237.76.86	navy.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
37.58.75.46	Netherlands	147.237.76.31	nakchal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
161.202.41.12	Netherlands	147.237.76.31	nakchal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
59.120.255.127	Taiwan	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
192.99.2.27	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
176.104.37.122	Ukraine	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.131	Italy	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.188	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
161.202.41.12	Netherlands	147.237.76.39	mobile.meitav.idf.il	C003: HTTP: phpMyAdmin access	Block	1
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
195.154.188.28	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
37.58.75.46	Netherlands	147.237.77.234	halag.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

12-01-2015 to 12-02-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.179.60.10	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	72
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	61
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	60
63.143.34.37	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	30
95.211.70.193	147.237.76.86	Netherlands	navy.idf.il	SQL Injection - Select From	26
74.84.136.105	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	24
189.38.90.144	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	23
211.23.251.92	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	21
46.19.85.29	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	21
23.91.70.63	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	10
103.21.58.191	147.237.77.74	India	law.idf.il	SQL Injection - Select From	10
46.19.85.149	147.237.0.19	Israel	madim.atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	8
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	8
62.90.76.231	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	5
195.154.216.86	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	4
171.232.56.152	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	4
195.154.216.86	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	4
195.154.216.86	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
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
171.232.56.152	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	4
59.120.255.127	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	3
197.165.237.19	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	3
197.165.237.19	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	3
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
150.164.225.30	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
195.154.188.28	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
195.154.211.20	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
195.154.188.28	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
66.249.66.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.154.211.20	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
80.250.148.225	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
209.126.116.147	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	2
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
66.102.9.6	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.18.141	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
31.6.71.154	147.237.77.216	Poland	dover.idf.il	ET SCAN NMAP -sS window 1024	2
195.154.211.20	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
195.154.211.20	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
114.112.90.54	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
31.6.71.154	147.237.76.34	Poland	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
195.154.188.28	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
66.249.66.28	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
195.154.188.224	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
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
134.191.232.72	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	2

12-01-2015 to 12-02-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.10.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2355
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1075
195.160.240.11	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	690
46.19.85.104	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	567
2.54.14.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	549
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	529
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	513
37.26.147.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	507
79.179.121.241	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	480
79.183.192.87	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
2.54.14.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	429
2.54.43.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	405
109.65.201.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	252
46.19.86.221	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	201
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	178
52.5.69.31	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	167
54.85.198.156	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	124
52.5.133.46	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	109
213.8.204.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	106
109.65.140.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	99
5.29.25.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	94
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	94
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
46.19.86.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	74
77.87.228.68	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	71
2.52.146.46	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	63
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	59
137.95.1.11	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	56
80.246.133.30	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	53
80.246.133.218	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
79.181.99.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
100.100.95.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	50
2.54.190.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
212.179.21.194	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.54.139.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	47
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	46
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	46
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
209.95.44.178	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
46.19.85.130	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
79.176.216.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	40
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	40
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	39
62.207.60.231	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	38
79.182.98.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
31.168.79.54	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
54.174.179.157	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	36

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.69.169	Block	860
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	621
2.54.10.197	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.10.197	Block	358
2.52.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	262
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	260
176.12.136.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	255
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	235
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.106.226.102	Block	202
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	201
176.13.2.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.2.210	Block	185
176.12.136.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.136.211	Block	177
85.65.63.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.63.136	Block	176
176.13.3.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	172
207.241.226.42	United States	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 207.241.226.42	Block	162
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
80.246.130.179	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
195.160.240.11	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 195.160.240.11	Block	119
85.65.63.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
2.52.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
5.29.25.143	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	108
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
62.219.153.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.2.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
79.177.35.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
176.13.2.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.2.210	Block	91
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.50	Block	87
46.19.85.104	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
37.26.148.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
174.64.97.238	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.4	Block	79
37.26.148.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
176.13.10.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
2.54.24.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
176.13.3.129	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.3.129	Block	75
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
95.86.107.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
176.13.21.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.106.226.102	Block	67
37.26.147.204	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
176.106.226.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
2.54.8.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
79.179.121.241	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
5.29.235.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
85.65.63.136	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.65.63.136	Block	54
207.241.226.41	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	54
37.26.148.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
46.117.103.25	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43