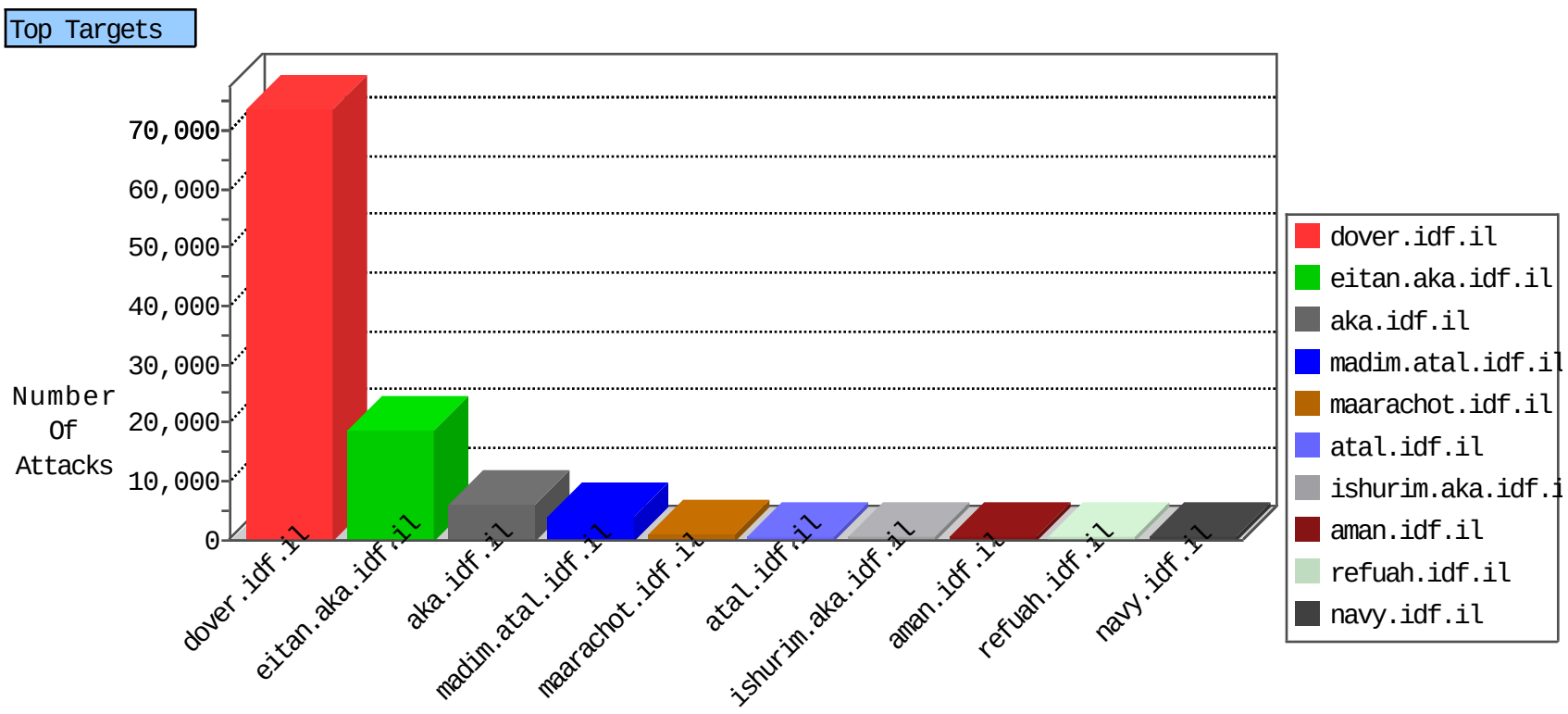
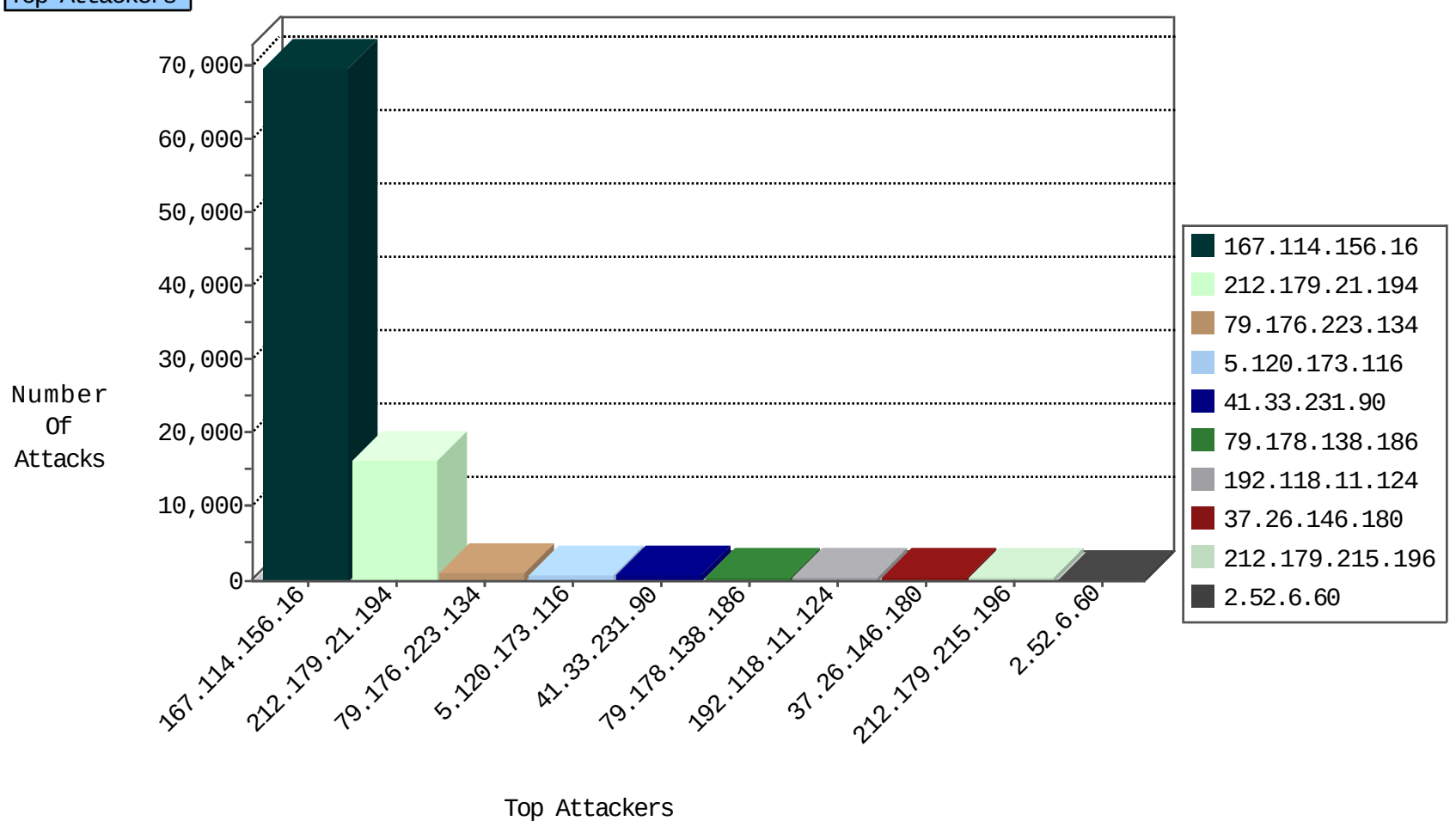
12-03-2015 to 12-04-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-03-2015 to 12-04-2015

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	90585
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2948
66.249.66.36	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1406
66.249.66.65	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1350
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1144
66.249.66.23	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	769
66.249.66.12	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	489
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	450
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	359
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	348
77.245.76.118	United Kingdom	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	186
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
91.197.62.30	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	32
2.54.153.120	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
109.66.59.144	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	24
69.42.220.26	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	11
79.183.145.154	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
70.167.141.55	United States	147.237.76.202	e.halag.idf.il	L4 Source or Dest Port Zero	drop	6
37.26.148.130	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
213.151.57.14	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
121.224.91.182	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	4
79.183.27.42	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
180.177.22.83	Taiwan	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	3
147.236.238.250	Israel	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	3
119.123.146.16	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	3
39.115.45.16	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
190.113.90.36	Guatemala	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
62.0.34.177	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
117.26.202.79	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
94.177.122.69	Romania	147.237.76.31	nakchal.idf.il	L4 Source or Dest Port Zero	drop	2
79.183.145.154	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
69.42.220.26	United States	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	2
124.130.148.254	China	147.237.76.38	e.e.meitav.idf.il	Invalid TCP Flags	drop	2
37.146.193.223	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
96.44.187.172	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
111.192.90.34	China	147.237.77.234	halag.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
94.177.122.69	Romania	147.237.76.34	yohalan.idf.il	L4 Source or Dest Port Zero	drop	2
203.255.19.62	Korea, Republic of	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.8	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
84.23.52.242	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.37	China	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
110.35.238.165	Korea, Republic of	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
31.129.115.109	Ukraine	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
94.158.39.128	Ukraine	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-03-2015 to 12-04-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.31.44.3	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
41.140.186.251	Morocco	147.237.77.216	dover.idf.il	12373: HTTP: WordPress admin Login	Block	12
87.242.112.36	Russian Federation	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
118.238.227.101	Japan	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
37.211.90.65	Qatar	147.237.77.216	dover.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	4
37.247.122.28	Spain	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
167.114.242.198	Canada	147.237.76.86	navy.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
192.187.121.66	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.150	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
105.103.248.100	Algeria	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
195.154.188.224	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
180.245.178.96	Indonesia	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
151.80.31.116	Italy	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
69.30.215.142	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.8.50	e.tikshuv.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
193.111.140.153	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
105.105.124.25	Algeria	147.237.77.216	dover.idf.il	3807: HTTP: SQL Injection Evasion Inline SQL Comment	Block	1
195.154.191.162	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.98	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.138	Italy	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
198.20.69.74	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
78.177.209.255	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
195.154.188.28	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
157.55.39.243	United States	147.237.77.226	www.chamatz.aka.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
195.154.194.59	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.117	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.142	Italy	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.35	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
62.210.152.89	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.211.20	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.117	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.150	Italy	147.237.76.86	navy.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

12-03-2015 to 12-04-2015

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	74
118.238.227.101	147.237.77.233	Japan	atal.idf.il	SQL Injection - Select From	24
64.31.44.3	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
95.211.70.193	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	10
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
77.245.76.118	147.237.77.170	United Kingdom	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	8
176.12.136.64	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
180.245.178.96	147.237.77.216	Indonesia	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	8
87.242.112.36	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	8
123.139.24.66	147.237.77.176	China	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
176.12.141.63	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.81.212	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.81	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.28	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
81.169.251.74	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
105.103.248.100	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	2
46.19.86.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
82.234.56.185	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.97	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
124.90.48.202	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
58.243.224.39	147.237.76.200	China	eitan.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
222.244.108.239	147.237.77.235	China	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
176.49.107.201	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
101.18.168.61	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
204.13.204.139	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
80.178.148.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.179.171.73	147.237.76.31	Hong Kong	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
60.166.244.147	147.237.77.176	China	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
169.54.233.117	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
2.54.138.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.160.150.62	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -f -sS	1
218.10.62.156	147.237.77.234	China	halag.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
87.66.80.152	147.237.0.19	Belgium	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.201	Moldova, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
177.124.125.217	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
42.92.135.48	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
122.128.36.250	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.204.188.142	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.47.14.226	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

12-03-2015 to 12-04-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.223.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	984
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	772
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	642
79.178.138.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	519
5.120.173.116	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	291
5.120.173.116	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	276
5.120.173.116	Iran, Islamic Republic of	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	275
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	189
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	156
37.26.149.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	110
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	96
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
193.17.232.2	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	90
109.201.154.162	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	86
94.230.84.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	81
212.199.34.114	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	78
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	78
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
80.246.130.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
100.100.10.184		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	63
46.19.86.42	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	59
100.100.1.245		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	56
37.19.120.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
46.19.85.14	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	53
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
185.26.182.29	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	44
37.26.148.178	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
46.19.86.82	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	43
77.125.74.113	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
213.57.138.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	39
213.57.138.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	36
212.179.215.196	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
195.151.206.228	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.85.61	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
85.64.4.30	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
95.86.99.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
109.226.28.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
100.100.116.203		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	32
176.106.40.250	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
209.216.220.173	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
145.225.60.5	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	30
46.32.200.145	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.12.150.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
199.203.196.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9552
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	5975
192.118.11.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 192.118.11.124	Block	281
37.142.68.87	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.68.87	Block	190
79.176.223.134	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	174
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	151
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	146
89.139.54.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	142
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.180	Block	139
213.57.61.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	130
2.52.6.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	122
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.154	Block	110
192.118.11.124	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	104
2.52.6.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
2.54.187.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
213.57.61.61	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 213.57.61.61	Block	99
192.118.11.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 192.118.11.124	Block	97
109.67.200.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
2.54.10.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.146.180	Block	90
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
176.13.5.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
2.52.6.60	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.52.6.60	Block	66
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
176.12.137.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
79.178.138.186	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
89.139.54.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	62
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	60
2.54.1.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
176.12.140.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
2.54.171.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
2.54.174.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
37.26.147.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
2.54.149.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
176.12.148.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.25.102.57	Block	41
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
37.26.147.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
176.13.15.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
176.12.149.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
176.12.139.49	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	35
176.12.139.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
2.52.33.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
176.12.143.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
2.54.51.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	29