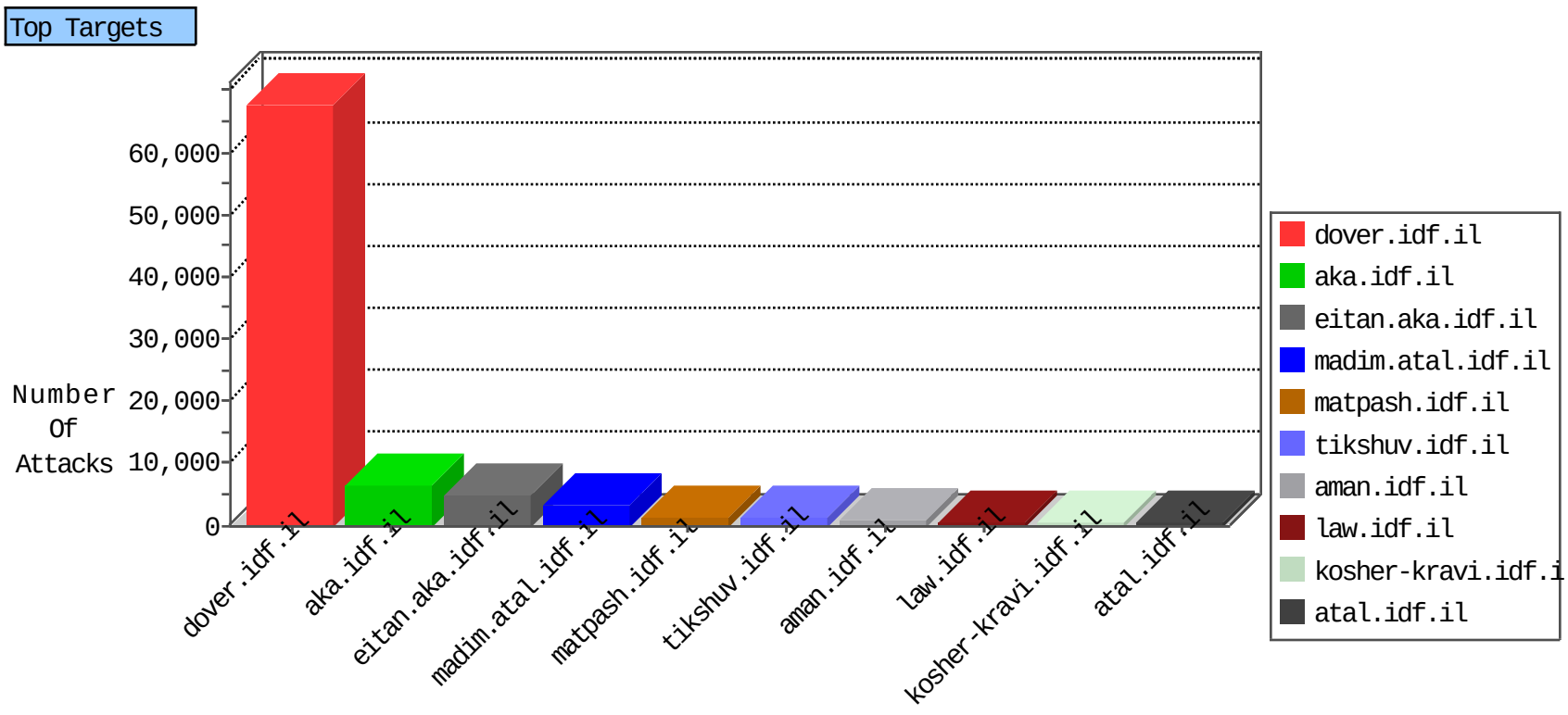
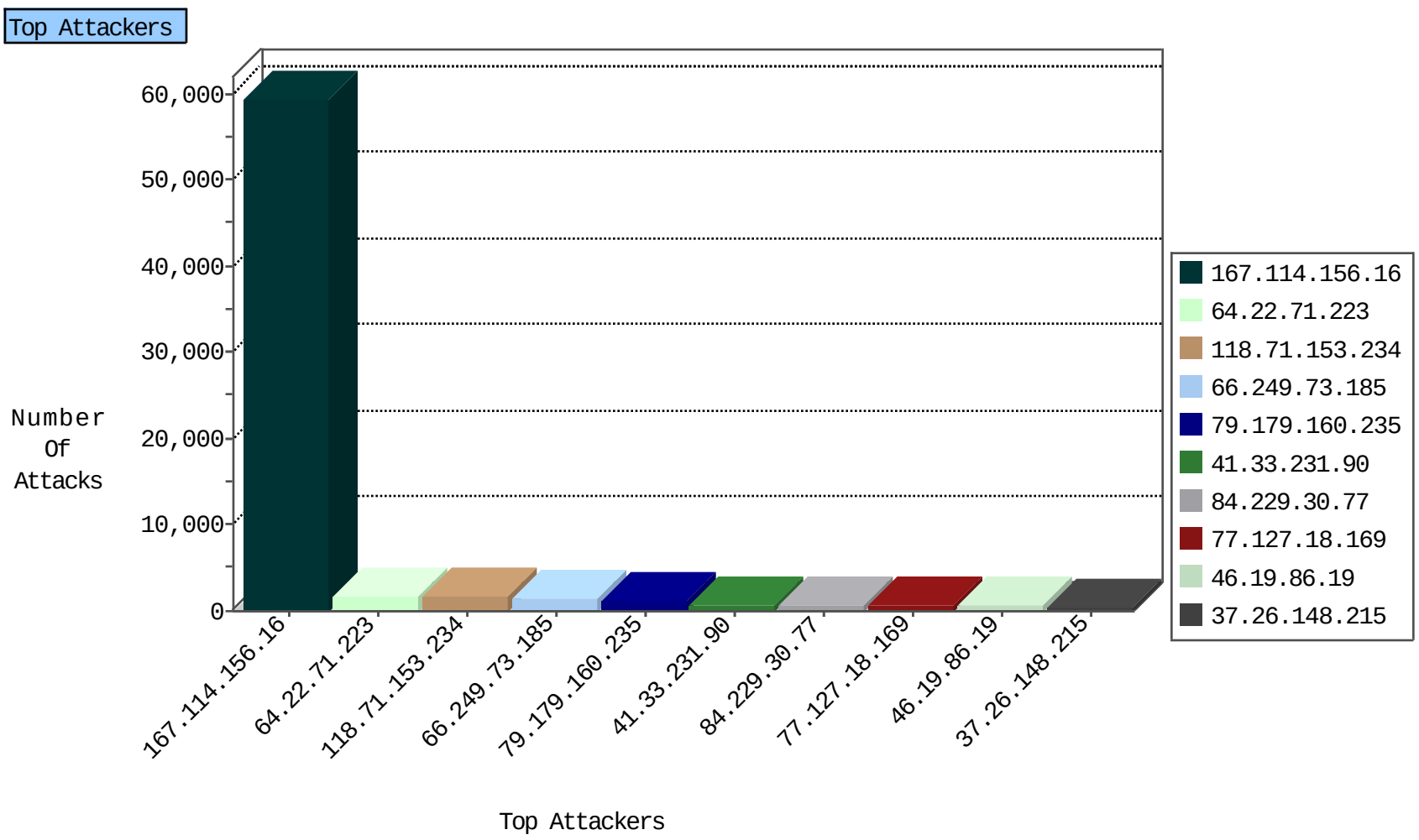
11-27-2015 to 11-28-2015

IDF Under Attack
Daily Report





11-27-2015 to 11-28-2015

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	90835
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	14246
66.249.66.125	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1219
66.249.75.106	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1103
66.249.66.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	776
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	626
82.145.216.94	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	32
168.235.197.173	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
66.249.66.39	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	22
79.180.225.62	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	14
79.176.205.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
37.48.65.47	Netherlands	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	8
79.182.128.109	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.183.14.170	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.180.58.69	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
58.51.90.38	China	147.237.77.234	halag.idf.il	L4 Source or Dest Port Zero	drop	5
85.65.199.219	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	5
64.22.71.223	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	4
35.0.127.52	United States	147.237.72.156	aman.idf.il	SYN Flood unverified cookie	drop	4
93.174.93.151	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
79.183.150.105	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
147.236.32.188	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.176.42.43	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
177.87.252.15	Brazil	147.237.77.235	sviva.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
200.29.186.163	Chile	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
153.31.160.5	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
177.136.184.55	Brazil	147.237.77.179	e.mazi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
113.17.175.198	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
59.61.46.197	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
180.111.221.186	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
168.235.197.173	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	2
115.231.222.40	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
37.57.154.139	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2

11-27-2015 to 11-28-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.77.233	atal.idf.il	C095: Suspicious Addresses MFA	Permit	39
45.59.196.109		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
45.59.196.109		147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
200.59.205.238	Argentina	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
93.172.23.131	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.251.252	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
194.114.146.227	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
81.218.251.250	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	5
109.67.27.70	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
89.26.241.213	Portugal	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	4
37.202.102.210	Jordan	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
41.142.202.55	Morocco	147.237.77.216	dover.idf.il	C1000158: HTTP(S): Hacked in the Payload	Block	2
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	2
188.165.15.160	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
89.139.15.115	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
91.218.29.20	Ukraine	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
182.50.130.134	Singapore	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
111.206.116.217	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
198.20.69.74	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
37.48.65.47	Netherlands	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1
136.243.73.82	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.240	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.120.159.150	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
198.245.62.10	Canada	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
89.31.57.5	Italy	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
151.80.31.142	Italy	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
95.91.45.195	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
86.121.112.161	Romania	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
192.99.2.137	Canada	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
188.165.15.50	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
115.42.137.250	Singapore	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
188.165.15.181	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.148.246	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
41.42.82.185	Egypt	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1
87.69.26.123	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
46.19.85.24	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
121.200.54.195	India	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
79.178.101.190	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.193	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
41.42.83.127	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
87.69.139.97	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.74	United States	147.237.8.50	e.tikshuv.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.64	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-27-2015 to 11-28-2015

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	94
118.71.153.234	147.237.77.216	Vietnam	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	52
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	42
200.59.205.238	147.237.77.233	Argentina	atal.idf.il	SQL Injection - Select From	24
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	17
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP backup access	14
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	10
66.249.81.164	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	10
118.71.153.234	147.237.77.176	Vietnam	matpash.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	9
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	8
89.26.241.213	147.237.77.74	Portugal	law.idf.il	Tehila - Perl LWP with fake user agent	8
118.71.153.234	147.237.77.233	Vietnam	atal.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	7
118.71.153.234	147.237.76.86	Vietnam	navy.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	6
41.142.202.55	147.237.77.216	Morocco	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
118.71.153.234	147.237.72.166	Vietnam	aka.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	5
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.75.106	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
85.65.132.175	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.73.185	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
118.71.153.234	147.237.77.74	Vietnam	law.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	4
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	4
118.71.153.234	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	4
118.71.153.234	147.237.76.200	Vietnam	eitan.aka.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	3
79.181.163.55	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
118.71.153.234	147.237.0.34	Vietnam	tikshuv.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	3
41.42.83.127	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	3
118.71.153.234	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	3
66.249.75.44	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
185.77.128.236	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
66.249.67.243	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
222.186.42.218	147.237.77.216	China	dover.idf.il	SERVER-WEBAPP JBoss JMXInvokerServlet access attempt	2
5.102.254.190	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	2
213.184.127.45	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP printenv access	2
116.24.250.31	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	2
218.24.171.223	147.237.76.177	China	ncore.idf.il	GPL SCAN nmap TCP	2
185.77.128.236	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
176.32.134.83	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	2
61.149.161.186	147.237.0.15	China	kosher-kravi.idf.il	GPL SCAN nmap TCP	2
185.77.128.236	147.237.0.34		tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
91.218.29.20	147.237.77.176	Ukraine	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
59.46.193.114	147.237.76.177	China	ncore.idf.il	GPL SCAN nmap TCP	2
66.249.93.231	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
177.87.252.15	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.134	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	2

11-27-2015 to 11-28-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1486
79.179.160.235	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1062
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	692
84.229.30.77	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	672
77.127.18.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	585
37.26.148.215	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	487
46.19.86.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	483
118.71.153.234	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	426
77.126.99.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	408
79.182.7.199	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	405
64.22.71.223	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	318
64.22.71.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	245
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	189
185.120.126.48		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	170
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	124
222.186.55.169	China	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	108
82.145.218.45	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	97
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
95.86.110.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
100.100.52.185		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
100.100.121.93		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	62
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
100.100.120.6		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	59
46.19.85.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	59
100.100.64.161		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	56
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
100.100.66.25		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	54
100.100.125.75		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	54
100.100.100.236		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	52
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
109.67.151.8	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
5.22.131.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	51
100.100.36.203		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	50
45.59.196.109		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
100.100.57.52		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	48
100.100.34.98		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	48
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.54.43.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	47
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
100.100.48.159		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	46
168.235.197.173	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
213.204.101.24	Lebanon	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	44
100.100.92.200		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	44
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
80.246.133.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
185.120.126.32		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	43

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
118.71.153.234	Vietnam	147.237.77.176	matpash.idf.il	Distributed Abnormally Long Request	Block	716
64.22.71.223	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 64.22.71.223	Block	592
64.22.71.223	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	267
79.179.160.235	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	218
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	193
149.88.228.56	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.228.56	Block	157
37.26.146.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	142
149.88.228.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
2.52.150.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	116
93.173.177.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.52.150.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
37.26.146.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.45	Block	104
31.168.164.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
80.246.137.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
93.173.6.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
31.168.164.230	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 31.168.164.230	Block	84
85.64.1.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
77.127.18.169	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.18.169	Block	84
79.178.196.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
109.64.218.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
79.179.24.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
2.54.21.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
2.52.141.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
93.172.9.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
79.178.196.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
176.12.148.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
176.13.3.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.86.19	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.19	Block	56
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	53
2.54.21.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
46.19.86.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
207.241.226.41	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	48
2.52.150.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	47
84.229.30.77	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.229.30.77	Block	44
185.120.126.72		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
185.32.179.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
109.160.253.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.13.19.115	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	38
37.142.68.74	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.68.74	Block	37
46.120.69.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.69.191	Block	36
118.71.153.234	Vietnam	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 118.71.153.234	Block	34
85.64.1.254	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.1.254	Block	34
46.120.229.186	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
79.182.7.199	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
80.246.133.111	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.133.111	Block	31