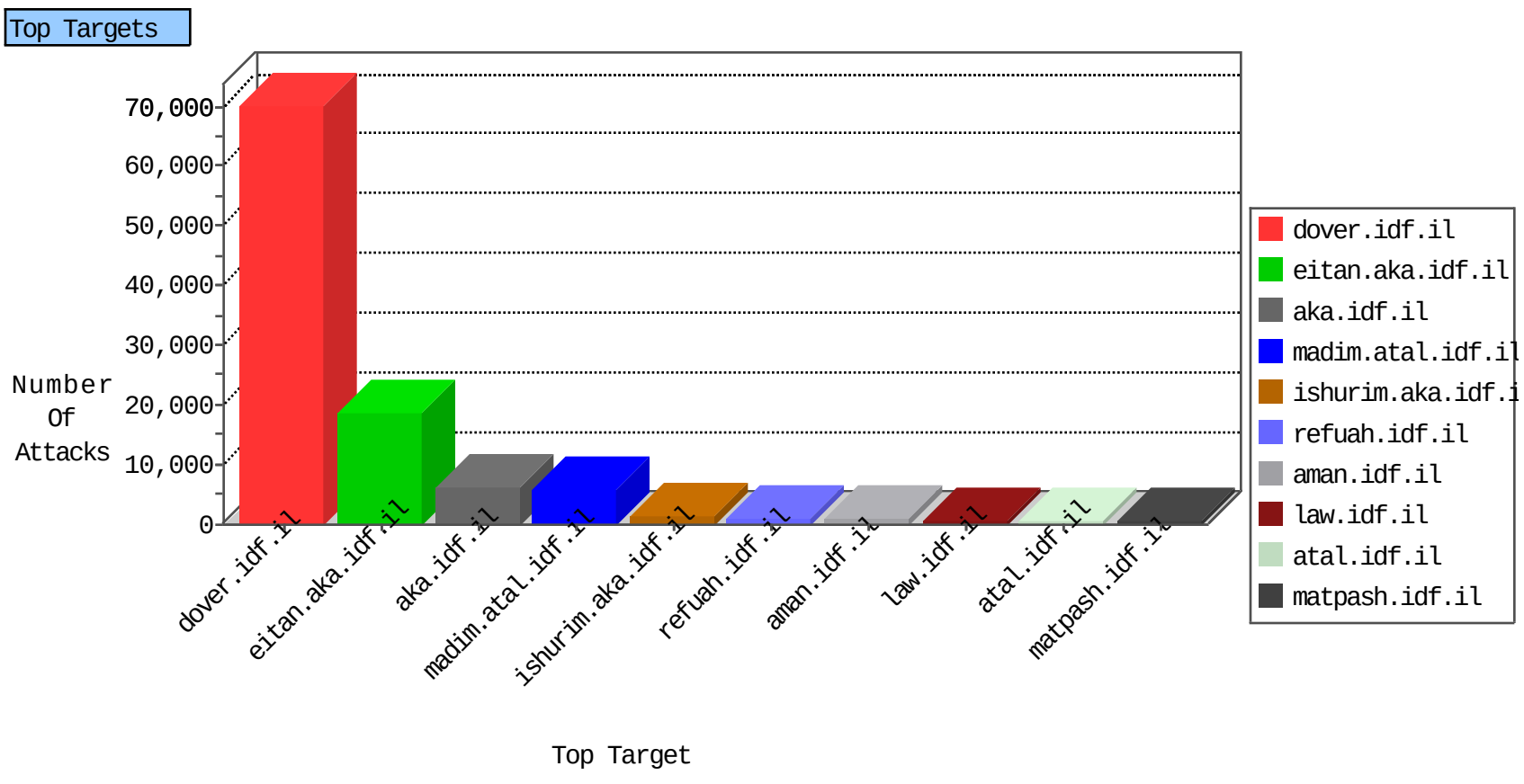
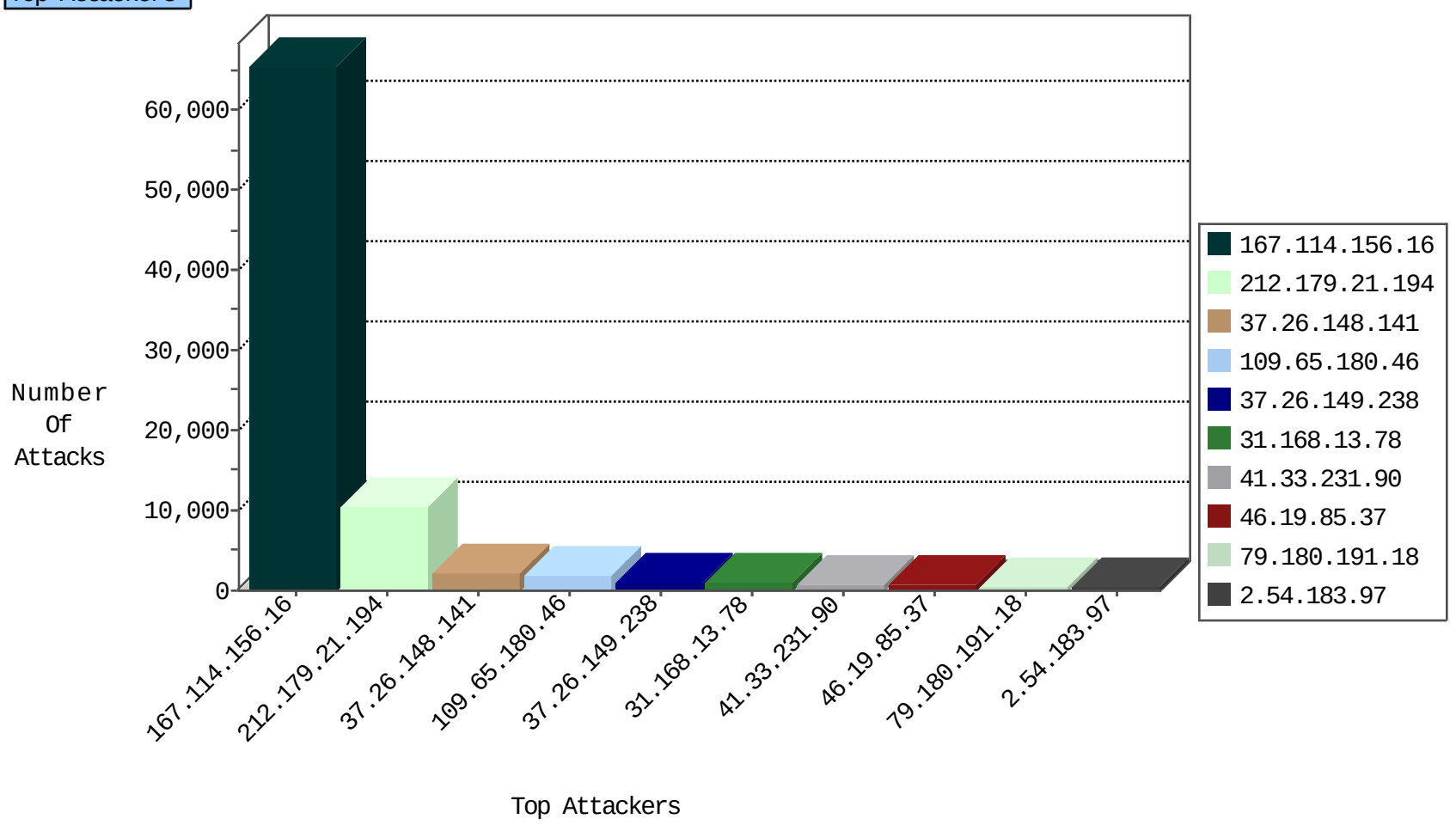
12-08-2015 to 12-09-2015

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-08-2015 to 12-09-2015

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	90837
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5165
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3121
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2862
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	578
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	506
66.249.66.1	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	357
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	319
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	241
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	93
134.191.232.69	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	82
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	48
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	40
134.191.232.69	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	32
168.235.196.156	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
45.32.246.5		147.237.76.198	e.yohalan.idf.il	Invalid TCP Flags	drop	12
45.32.246.5		147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	12
45.32.246.5		147.237.76.197	e.himush.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	8
79.176.206.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
176.189.203.143	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
94.123.202.49	Turkey	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.109.12.233	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
45.32.246.5		147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	6
45.32.246.5		147.237.76.200	eitan.aka.idf.il	Invalid TCP Flags	drop	6
176.13.9.11	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
45.32.246.5		147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	4
45.32.246.5		147.237.77.121	e.navy.idf.il	Invalid TCP Flags	drop	3
79.178.0.129	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
45.32.246.5		147.237.8.45	e.eitan.idf.il	Invalid TCP Flags	drop	3
37.204.108.17	Russian Federation	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	3
79.178.211.119	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.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
79.176.36.4	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
123.151.42.61	China	147.237.76.31	nakchal.idf.il	JLM_Purple_Con_Limit_Udp	drop	3
93.174.93.138	Netherlands	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
167.114.242.197	Canada	147.237.77.226	www.chamatz.aka.idf.il	Frk_Under_Attack_Con_Https	drop	2
220.163.110.126	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.8	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
123.151.42.61	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Udp	drop	2
201.205.51.21	Costa Rica	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
183.60.48.25	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
168.235.196.156	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	2
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
205.203.135.1	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
45.32.246.5		147.237.72.217	e.idf.il	Invalid TCP Flags	drop	2
37.204.108.17	Russian Federation	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
115.231.222.40	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2

12-08-2015 to 12-09-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.47.2.10	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
158.85.253.245	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
50.97.138.113	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	14
168.63.12.166	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	9
108.168.219.166	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
96.47.2.10	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
50.97.138.113	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
93.89.16.110	Turkey	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
178.63.18.196	Germany	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
158.85.253.245	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
37.59.56.6	France	147.237.77.216	dover.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	4
168.63.12.166	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
50.97.138.113	United States	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	2
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
210.48.147.115	Malaysia	147.237.77.216	dover.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
185.106.94.91		147.237.76.42	refuah.idf.il	C003: HTTP: phpMyAdmin access	Block	1
158.85.253.245	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
200.98.137.169	Brazil	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
37.59.56.6	France	147.237.77.216	dover.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
185.106.94.91		147.237.72.166	aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
222.106.222.148	Korea, Republic of	147.237.72.166	aka.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
185.106.94.91		147.237.76.86	navy.idf.il	C003: HTTP: phpMyAdmin access	Block	1
167.114.242.197	Canada	147.237.77.226	www.chamatz.aka.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
208.52.161.177	United States	147.237.0.19	madim.atal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
185.106.94.91		147.237.76.30	himush.idf.il	C003: HTTP: phpMyAdmin access	Block	1
149.202.44.111	Germany	147.237.77.170	maarachot.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
78.46.174.197	Germany	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
185.106.94.91		147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1
208.52.161.177	United States	147.237.77.205	prisha.idf.il	C003: HTTP: phpMyAdmin access	Block	1
185.106.94.91		147.237.76.31	nakchal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
91.121.74.44	France	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.148	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
208.52.161.177	United States	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1
185.106.94.91		147.237.76.39	mobile.meitav.idf.il	C003: HTTP: phpMyAdmin access	Block	1
198.20.69.74	United States	147.237.76.199	e.nakchal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
5.9.140.208	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

12-08-2015 to 12-09-2015

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	75
41.185.31.40	147.237.76.42	South Africa	refuah.idf.il	SQL Injection - Select From	54
50.97.138.113	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	43
23.91.70.94	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	34
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	32
96.47.2.10	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	26
168.63.12.166	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	15
184.168.193.34	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
31.168.151.101	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	14
93.89.16.110	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	13
176.106.230.79	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	11
108.168.219.166	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
81.218.176.159	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	10
178.63.18.196	147.237.77.74	Germany	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	8
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	8
37.59.56.6	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	5
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	4
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
162.216.46.37	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	3
213.246.49.97	147.237.0.34	France	tikshuv.idf.il	SQL Injection - Select From	3
66.249.64.200	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
212.179.132.202	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
162.216.46.37	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.88.46	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.135	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
85.64.207.163	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.22	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
176.12.136.76	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
37.142.192.91	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.45	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
162.216.46.37	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.81.196	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
43.225.68.247	147.237.8.28	Japan	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
66.249.80.105	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	2
176.12.136.76	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
66.249.66.39	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
109.186.19.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.79.208.148	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential SSH Scan	1
199.168.136.165	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.36	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
124.74.213.36	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.182.163.75	147.237.76.39	Iran, Islamic Republic of	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1

12-08-2015 to 12-09-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.180.46	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1563
37.26.148.141	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1398
37.26.149.238	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	840
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	753
79.180.191.18	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	504
2.54.183.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	441
84.228.176.11	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	402
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	356
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	301
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	202
62.103.30.184	Greece	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	178
80.178.204.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	171
80.246.133.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	141
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	134
79.178.191.226	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	102
46.19.86.210	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	97
79.178.191.226	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
5.29.223.67	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	86
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
2.54.63.148	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
79.180.194.219	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
109.66.139.227	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
109.64.21.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	51
46.224.175.21	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
79.181.231.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
84.228.213.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
89.138.94.219	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
198.240.213.23	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	49
85.130.201.81	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	48
79.178.191.226	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	45
113.161.8.164	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
46.19.85.90	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
2.54.55.165	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
46.224.175.21	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	33
46.19.85.151	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
134.191.232.69	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	31
46.19.85.26	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
95.35.236.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
168.235.196.156	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
213.8.63.243	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	30
46.19.85.252	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
2.52.55.49	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29

12-08-2015 to 12-09-2015

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
199.30.25.213	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
31.168.211.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	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	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	6477
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3562
31.168.13.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 31.168.13.78	Block	564
109.65.180.46	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	416
66.158.58.200	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	396
37.26.148.141	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	374
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
37.26.148.141	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.141	Block	313
193.104.115.2	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 193.104.115.2	Block	287
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	269
5.29.223.67	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	256
31.168.13.78	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 31.168.13.78	Block	226
109.65.209.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	178
37.26.149.238	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	176
176.13.12.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	170
79.176.109.24	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.109.24	Block	167
176.13.23.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
2.52.158.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.158.90	Block	145
84.108.249.195	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.108.249.195	Block	145
37.142.176.208	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.176.208	Block	142
176.13.12.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
79.176.109.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
2.52.158.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	121
176.13.18.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
85.250.69.178	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	118
109.65.209.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.62	Block	117
31.168.13.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
37.142.176.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.4.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
149.78.57.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
176.13.23.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
212.199.70.130	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
2.54.166.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
207.241.226.41	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	68
193.10.72.205	Sweden	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.10.72.205	Block	66
98.7.94.168	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
176.12.139.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
79.180.191.18	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.191.18	Block	63
65.30.210.222	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
79.176.109.24	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 79.176.109.24	Block	58