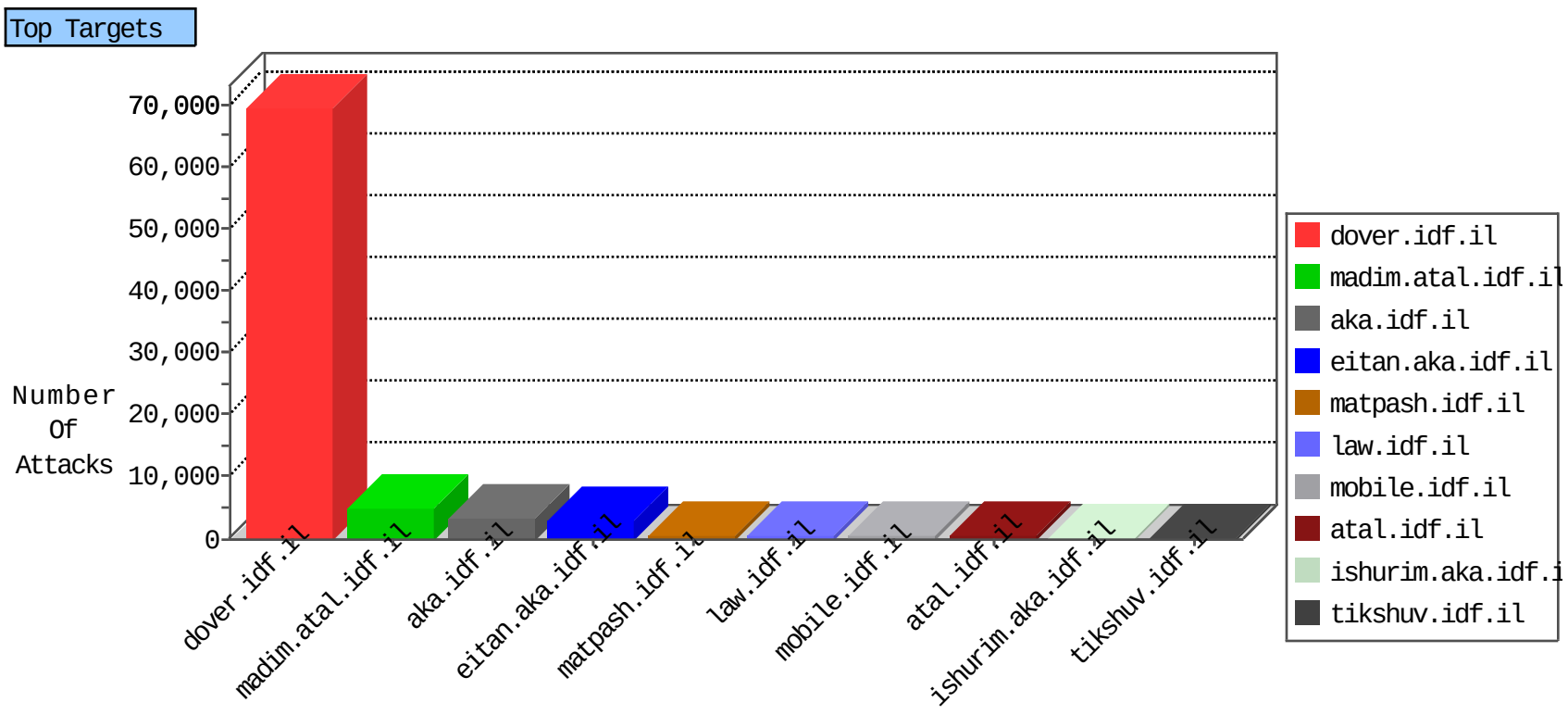
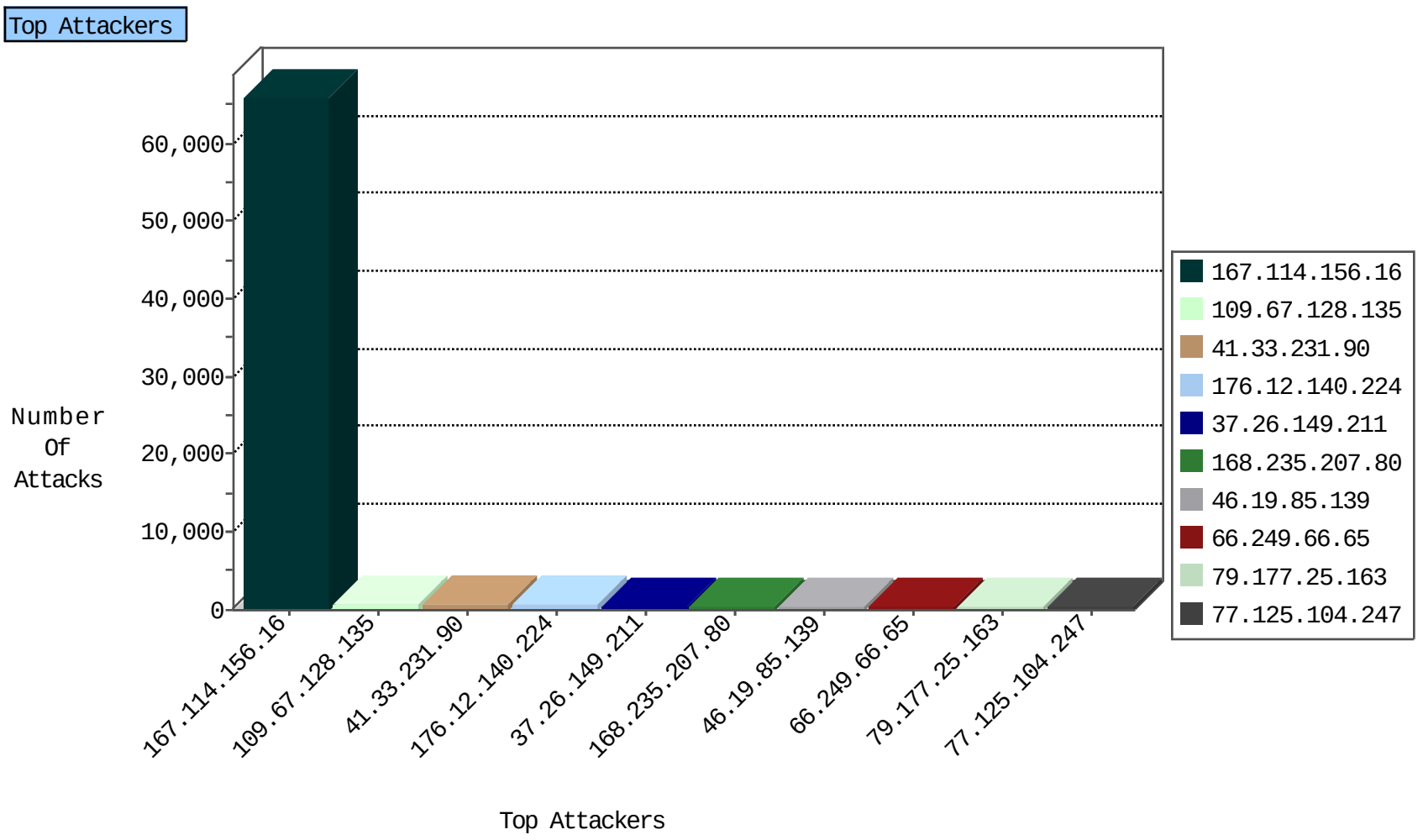
12-11-2015 to 12-12-2015

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-11-2015 to 12-12-2015

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	89780
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3164
41.107.58.176	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	79
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	55
168.235.201.49	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
8.37.231.51	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
66.249.79.3	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	21
79.176.19.20	Israel	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	16
109.67.107.19	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
41.107.58.176	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
151.0.151.137	Romania	147.237.8.28	e.mobile-ks.idf.il	L4 Source or Dest Port Zero	drop	4
168.235.207.80	United States	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
79.176.197.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
188.138.33.34	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	3
93.173.136.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.201.116	United States	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
109.67.107.68	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
149.88.190.136	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
84.229.132.170	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
8.37.231.51	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
94.102.49.210	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
168.235.201.49	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	2
94.102.49.210	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
94.102.49.210	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
183.196.130.141	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
94.102.49.210	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
116.55.222.99	China	147.237.77.243	mobile.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
95.46.194.200	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	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
94.102.49.210	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
94.102.49.210	Netherlands	147.237.76.31	nakchal.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
94.102.49.210	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
94.102.49.210	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
168.235.207.80	United States	147.237.77.176	matpash.idf.il	Frk_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
94.102.49.210	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
94.102.49.210	Netherlands	147.237.76.34	yohalan.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
222.186.50.254	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.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
94.102.49.210	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
93.174.93.68	Netherlands	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
60.189.70.32	China	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2

12-11-2015 to 12-12-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
61.183.118.225	China	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
61.183.118.225	China	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
151.80.31.143	Italy	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.144	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.78	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.35.180.112	United States	147.237.77.170	maarachot.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
94.75.220.155	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.35.187.114	United States	147.237.77.235	sviva.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
69.12.70.34	United States	147.237.77.19	law-forum.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
223.73.45.66	China	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
52.35.180.120	United States	147.237.76.31	nakchal.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
151.80.31.110	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
94.75.220.155	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
61.183.118.225	China	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
158.69.213.39	United States	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	1
51.254.121.187	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
109.67.146.72	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
69.12.70.34	United States	147.237.77.226	www.chamatz.aka.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
52.35.180.120	United States	147.237.76.86	navy.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
151.80.31.117	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
94.75.220.155	Netherlands	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
52.33.106.123	United States	147.237.72.167	ishurim.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
118.98.104.21	Indonesia	147.237.77.216	dover.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1
69.12.70.34	United States	147.237.77.235	sviva.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
52.35.180.120	United States	147.237.77.205	prisha.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
151.80.31.137	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
61.183.118.225	China	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
188.165.15.5	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.35.180.112	United States	147.237.0.19	madim.atal.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
123.125.125.77	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
69.30.214.42	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
52.35.187.114	United States	147.237.76.30	himush.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1

12-11-2015 to 12-12-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.65	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	516
46.19.85.99	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	120
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	93
80.246.130.199	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	13
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
37.26.149.211	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	6
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	5
80.246.130.56	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.79.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.79.6	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
109.64.126.254	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
84.19.178.10	147.237.77.216	Germany	dover.idf.il	Tehila - Perl LWP with fake user agent	3
213.151.32.163	147.237.72.166	Israel	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
202.113.77.254	147.237.0.35	China	akaws.idf.il	GPL SCAN nmap TCP	2
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
82.205.115.81	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
185.111.76.132	147.237.77.243		mobile.idf.il	ET SCAN Potential SSH Scan	2
113.106.129.219	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	2
66.249.79.3	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
46.151.208.247	147.237.77.216	Saudi Arabia	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
199.19.105.111	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
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
138.186.92.212	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	2
204.45.15.186	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
45.32.24.122	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	2
64.233.172.201	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
138.186.92.212	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	2
193.5.216.100	147.237.77.176	Switzerland	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.218	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.111.76.132	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	2
138.186.92.212	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	2
185.111.76.132	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	2
46.151.209.157	147.237.77.216	Saudi Arabia	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
66.249.66.184	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
212.179.177.148	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
185.111.76.132	147.237.0.15		kosher-kravi.idf.i	ET SCAN Potential SSH Scan	2
123.150.255.194	147.237.0.35	China	akaws.idf.il	GPL SCAN nmap TCP	2
221.238.82.194	147.237.0.35	China	akaws.idf.il	GPL SCAN nmap TCP	2
66.249.66.5	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
60.30.204.2	147.237.0.35	China	akaws.idf.il	GPL SCAN nmap TCP	2
45.32.24.122	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.108.132.58	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.68	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
193.104.41.54	147.237.0.34	Moldova, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

12-11-2015 to 12-12-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	808
109.67.128.135	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	711
168.235.207.80	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	500
46.19.85.139	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	462
79.177.25.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
77.125.104.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	197
85.65.46.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	168
79.182.185.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	104
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	87
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
168.235.201.49	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
8.37.231.51	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	67
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
104.131.221.26	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
213.57.134.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	56
213.57.141.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
213.57.134.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
195.182.151.246	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.85.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
46.19.86.182	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	40
46.19.85.25	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	40
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	40
46.19.86.111	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
46.19.85.226	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
70.210.78.160	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
213.57.131.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
213.57.131.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33
46.19.86.63	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	31
213.57.128.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
100.100.16.12		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
79.178.236.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.26.149.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
77.239.224.35	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
46.19.86.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.182.122.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.117.205.212	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
213.57.128.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
118.175.167.43	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
109.64.223.90	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.54.186.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
141.0.14.161	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.211	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.149.211	Block	334
176.12.140.224	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.140.224	Block	317
176.12.140.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	243
176.12.138.43	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.138.43	Block	230
195.182.151.246	Russian Federation	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	227
37.26.149.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	201
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.110.32.173	Block	189
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	169
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
207.241.226.39	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	134
46.19.85.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	134
79.181.137.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
109.67.128.135	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.67.128.135	Block	119
176.12.137.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
217.132.44.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
185.32.179.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
84.228.6.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.12.138.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
5.29.132.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
176.12.139.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
80.246.136.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
217.132.44.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	79
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 84.110.32.173	Block	72
46.19.85.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	71
176.13.6.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
207.241.226.39	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.39	Block	61
176.12.139.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	61
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
176.13.12.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.54.174.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
80.246.136.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
185.32.179.67	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.179.67	Block	54
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
46.19.85.139	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
176.12.140.224	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.12.140.224	Block	48
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
79.177.25.163	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
176.12.137.180	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.137.180	Block	43
2.52.16.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
37.26.146.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
176.13.6.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
77.125.104.247	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
2.54.144.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
5.29.132.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
176.12.146.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.54.152.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30