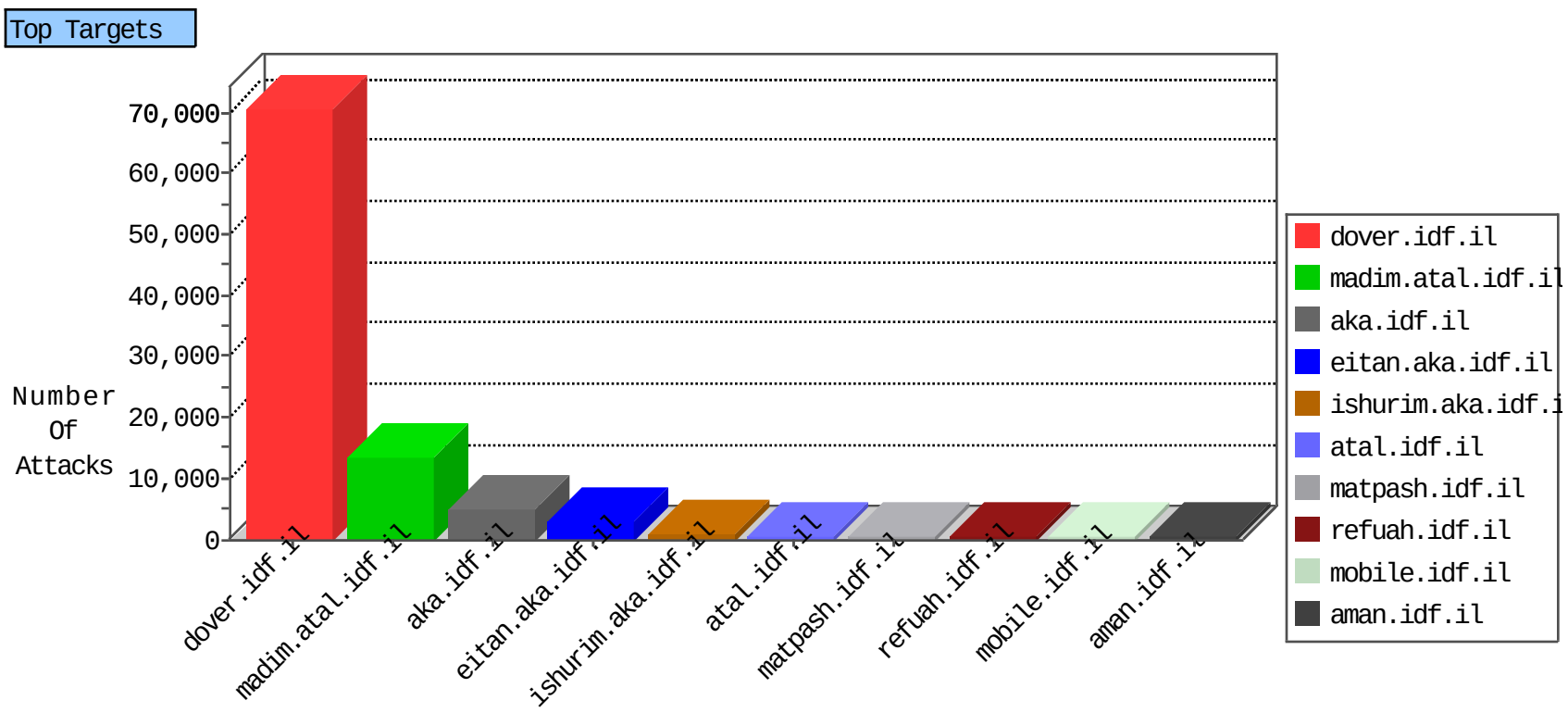
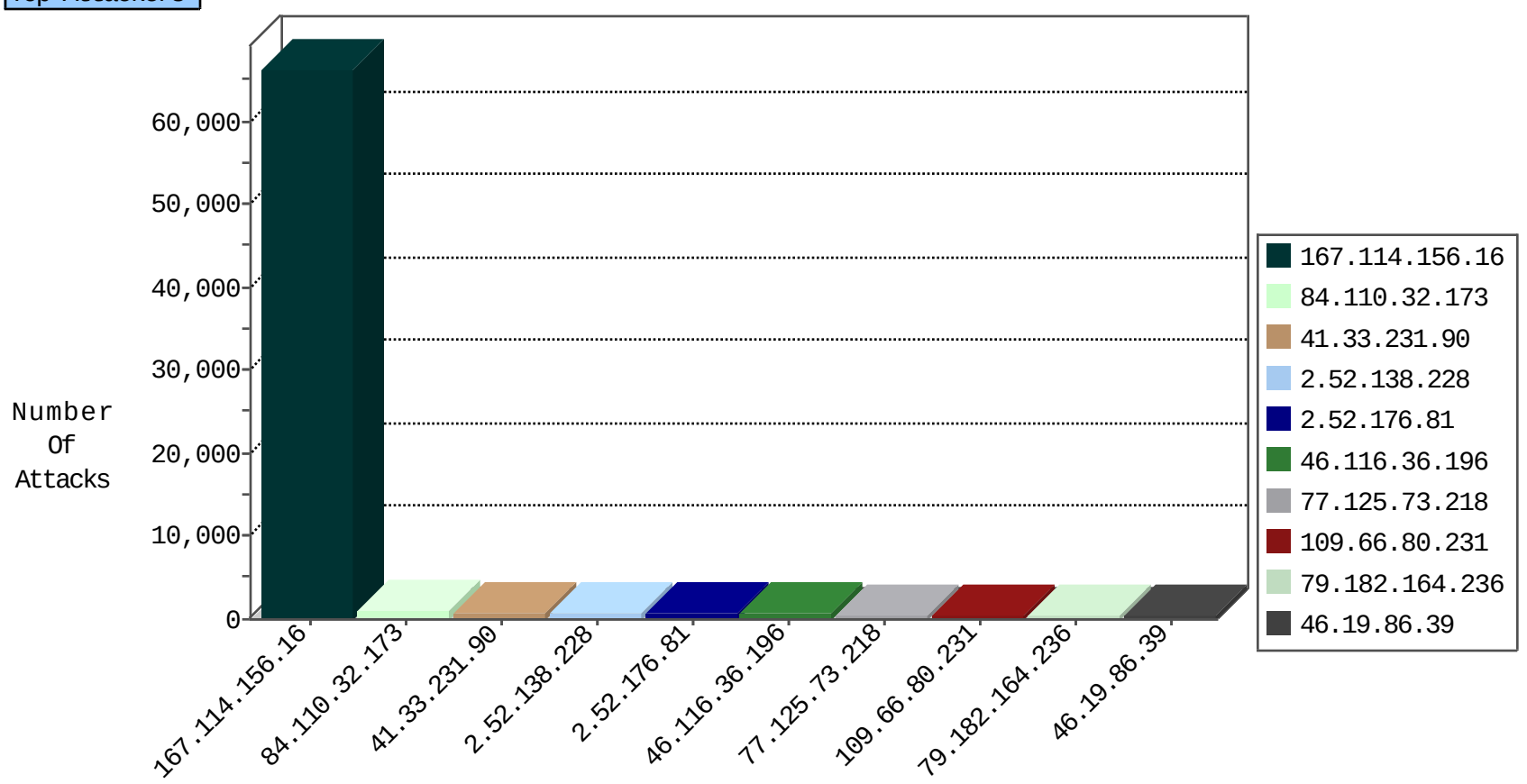
12-10-2015 to 12-11-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-10-2015 to 12-11-2015

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	90654
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	12172
66.249.79.10	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3088
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1174
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	330
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	303
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	107
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	106
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	56
109.67.113.97	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	34
2.52.143.237	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
45.32.246.5		147.237.77.74	law.idf.il	Invalid TCP Flags	drop	9
45.32.246.5		147.237.76.148	gqcenter.aka.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.34	yohalan.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.147	chinuch.aka.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.8.50	e.tikshuv.idf.il	Invalid TCP Flags	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
84.110.7.234	Israel	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	6
84.110.7.234	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
45.32.246.5		147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	6
216.165.95.1	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.54.16.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
5.133.30.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
45.32.246.5		147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	4
45.32.246.5		147.237.77.170	maarachot.idf.il	Invalid TCP Flags	drop	4
115.231.222.40	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	4
176.14.85.246	Russian Federation	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	3
45.32.246.5		147.237.77.205	prisha.idf.il	Invalid TCP Flags	drop	3
81.218.105.235	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.7	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
169.231.53.86	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
45.32.246.5		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
45.32.246.5		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
46.35.241.178	Russian Federation	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	3
213.57.182.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.151.55.116	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.8	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
98.209.136.30	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
50.4.163.157	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
66.151.55.110	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
113.163.237.199	Vietnam	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.151.55.117	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
66.151.55.112	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
176.14.85.246	Russian Federation	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Http	drop	2

12-10-2015 to 12-11-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	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
185.106.94.2		147.237.77.233	atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.106.94.2		147.237.72.156	aman.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.106.94.2		147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.106.94.2		147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	3
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
69.12.70.34	United States	147.237.76.31	nakchal.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
52.35.180.120	United States	147.237.76.39	mobile.meitav.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
81.17.21.234	Switzerland	147.237.0.34	tikshuv.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
52.35.187.114	United States	147.237.72.166	aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
188.165.15.224	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.33.106.123	United States	147.237.77.176	matpash.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
118.238.1.113	Japan	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
69.12.70.34	United States	147.237.76.200	eitan.aka.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
186.213.19.210	Brazil	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
52.35.180.120	United States	147.237.76.42	refuah.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
46.4.32.75	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
167.114.229.245	Canada	147.237.76.42	refuah.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
52.35.187.114	United States	147.237.77.234	halag.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
193.111.140.153	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.106.94.2		147.237.76.30	himush.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
52.33.106.123	United States	147.237.77.216	dover.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
69.30.234.2	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.43	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.35.180.120	United States	147.237.76.147	chinuch.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
46.118.118.215	Ukraine	147.237.76.86	navy.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
185.106.94.2		147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
69.12.70.34	United States	147.237.0.34	tikshuv.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
52.33.106.123	United States	147.237.77.226	www.chamatz.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
144.76.44.138	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
81.17.21.234	Switzerland	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
52.35.180.120	United States	147.237.76.200	eitan.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
188.165.15.84	France	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.252.131.34	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
112.111.188.201	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
69.12.70.34	United States	147.237.72.156	aman.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
212.83.178.132	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.106.94.2		147.237.77.233	atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
52.35.180.112	United States	147.237.72.156	aman.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
151.80.31.147	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
81.17.21.234	Switzerland	147.237.0.19	madim.atal.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
52.35.180.120	United States	147.237.77.233	atal.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
188.165.15.205	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
185.106.94.2		147.237.72.156	aman.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
112.111.188.201	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1

12-10-2015 to 12-11-2015

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	65
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	14
2.52.7.119	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	9
104.207.226.49	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP backup access	5
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
217.77.220.195	147.237.77.216	Ukraine	dover.idf.il	Tehila - Perl LWP with fake user agent	4
203.151.93.164	147.237.76.42	Thailand	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.74.109	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
213.242.62.166	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.60	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
80.246.130.172	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.102.9.6	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.81.183	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
46.151.211.227	147.237.77.216	Saudi Arabia	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
66.249.79.14	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.74.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.9	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
213.242.62.166	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	2
113.240.250.155	147.237.77.234	China	halag.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.79.127	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
201.53.249.82	147.237.77.233	Brazil	atal.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
94.75.220.155	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
101.227.249.242	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
212.76.104.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.21.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.102.229.196	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.121.203.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
162.251.167.74	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.24.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.160.150.62	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
213.242.62.166	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.213	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.53.249.82	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
181.66.43.248	147.237.0.17	Peru	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.76.86		navy.idf.il	ET SCAN NMAP -f -sS	1
138.94.34.136	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.71	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.246.5	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 3072	1
138.94.34.136	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

12-10-2015 to 12-11-2015

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	812
109.66.80.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	489
79.182.164.236	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	483
79.182.32.184	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	447
37.26.149.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
149.78.162.248	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	231
2.52.143.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	172
176.14.85.246	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	136
79.178.21.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	125
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
194.170.74.98	United Arab Emirates	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	90
213.57.128.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	75
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	73
213.57.128.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	73
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	68
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
213.57.128.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	55
207.232.37.138	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	52
37.26.149.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	47
212.143.231.14	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
169.231.53.86	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	46
109.65.106.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
212.179.102.173	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
87.69.37.73	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	41
100.100.16.12		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	41
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
158.169.150.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	39
2.54.50.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
2.54.28.27	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
46.19.85.212	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
77.126.27.187	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
148.177.129.212	Europe	147.237.72.166	aka.idf.il	drop	SAM rule	drop	34
80.246.130.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
2.52.143.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
62.207.60.231	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	32
78.144.68.71	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
93.173.171.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
5.28.155.154	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
185.120.125.21		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.179.119.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
5.28.156.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
158.169.150.10	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	29
148.177.129.212	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
93.173.14.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	533
2.52.176.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	433
46.116.36.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	387
77.125.73.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	318
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	272
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	246
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.138.228	Block	238
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	237
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	227
37.26.148.253	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.148.253	Block	222
84.109.118.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	222
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	220
77.125.73.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	213
85.64.181.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	192
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	192
176.13.14.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	186
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	185
2.52.138.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	185
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	184
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	181
46.120.61.143	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.61.143	Block	180
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	180
84.111.189.161	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.111.189.161	Block	179
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.111	Block	178
2.52.176.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	173
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
46.116.36.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	170
185.32.179.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	169
2.54.54.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
176.12.137.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	153
176.13.17.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	148
2.52.176.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	148
176.13.17.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	147
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.146.211	Block	147
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	146
2.54.174.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	138
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
2.54.54.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	127
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.89	Block	125
176.13.23.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	125
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	124
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
109.64.170.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	112
37.26.148.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
84.109.118.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	110
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109