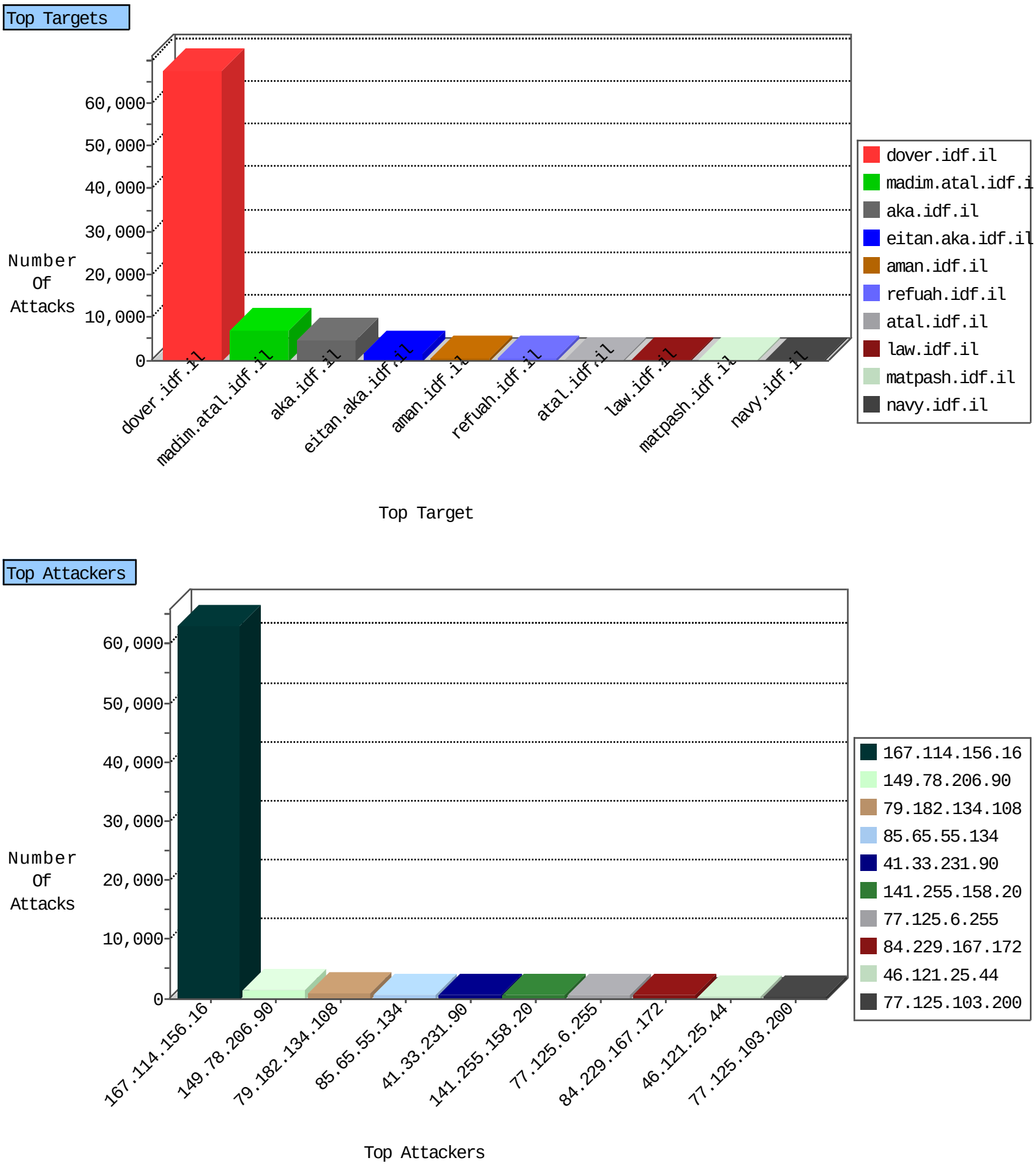
12-05-2015 to 12-06-2015

IDF Under Attack
Daily Report



12-05-2015 to 12-06-2015

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	90292
141.255.158.20	Netherlands	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	16343
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11279
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3237
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	764
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	509
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	333
66.249.64.165	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	202
134.191.232.69	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	100
149.88.142.57	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
66.249.64.186	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	52
134.191.232.69	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	50
190.189.249.156	Argentina	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	42
168.235.207.129	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
83.175.203.74	Spain	147.237.76.42	refuah.idf.il	L4 Source or Dest Port Zero	drop	7
84.109.112.159	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.109.112.159	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
104.131.199.242	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
199.59.148.210	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
168.235.207.129	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.145.210.6	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	4
108.168.47.213	Canada	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	3
188.161.58.16	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.65.215.149	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
173.252.120.101	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
199.30.24.224	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
146.185.57.7	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.0.163.75	Canada	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	3
95.35.194.137	Israel	147.237.72.166	aka.idf.il	block-sp-traf1	drop	3
61.233.104.12	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
2.132.232.85	Kazakstan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.249.92.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
94.102.56.238	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
222.186.21.75	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
14.167.175.121	Vietnam	147.237.77.234	halag.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
222.186.21.92	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
168.235.207.129	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
66.249.66.28	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.8	China	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
107.150.20.53	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

12-05-2015 to 12-06-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.44.192.77	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
68.64.161.3	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
113.67.169.128	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
93.63.188.181	Italy	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
68.64.161.3	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
173.44.192.77	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12
113.67.169.128	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
94.102.153.58	United Kingdom	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
93.63.188.181	Italy	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
195.234.228.90	Germany	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
222.84.7.172	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
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	147.237.77.176	matpash.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
198.20.69.74	United States	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
1.192.97.205	China	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
136.243.5.87	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
91.121.211.59	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.181	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
162.210.196.129	United States	147.237.77.176	matpash.idf.il	C1000106: HTTP: majestic bot	Block	1
105.158.68.33	Morocco	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
69.30.215.122	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
198.204.243.114	United States	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.13	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
136.243.73.82	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.193	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1
78.135.79.101	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
203.87.119.8	Australia	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.26	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
50.7.213.42	Czech Republic	147.237.77.233	atal.idf.il	C1000196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
167.114.242.197	Canada	147.237.76.31	nakchal.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
80.93.90.96	France	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
188.165.15.98	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
51.255.36.86	United Kingdom	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
144.76.44.138	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
94.102.56.143	Netherlands	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
69.12.70.34	United States	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
222.106.222.147	Korea, Republic of	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
80.93.90.96	France	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
188.165.15.117	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
158.69.214.109	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

12-05-2015 to 12-06-2015

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	96
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	26
93.63.188.181	147.237.72.166	Italy	aka.idf.il	SQL Injection - Select From	24
94.102.153.58	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	24
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	16
66.249.66.75	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	12
195.234.228.90	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	8
46.228.207.18	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.14	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	6
46.228.207.18	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
46.228.207.18	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
46.228.207.18	147.237.76.148	Germany	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
46.228.207.18	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
46.228.207.18	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
46.228.207.18	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
46.228.207.18	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
46.228.207.18	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
46.228.207.18	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
46.228.207.18	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
46.228.207.18	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
80.246.133.74	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	3
46.228.207.18	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
113.240.250.155	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
113.240.250.155	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
46.228.207.18	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
113.240.250.155	147.237.76.177	China	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
46.228.207.18	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.93.205	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
113.240.250.155	147.237.76.42	China	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
113.240.250.155	147.237.76.39	China	mobile.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
138.255.66.227	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
122.114.17.100	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.62	147.237.76.31	Israel	nakchal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.25	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	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
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	2
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
138.255.66.227	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2

12-05-2015 to 12-06-2015

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	716
77.125.6.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	591
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	425
37.26.146.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	303
213.8.204.47	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	166
37.26.146.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	159
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
213.57.133.198	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	74
213.57.128.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	72
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	67
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	55
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
109.67.198.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
80.246.130.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
31.154.171.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
92.90.17.93	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	38
213.8.204.36	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
37.142.68.68	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
31.154.171.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
79.178.38.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
80.246.133.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
188.48.9.209	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
37.26.146.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.246.133.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
79.181.25.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
166.172.58.253	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	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
66.87.78.99	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	26
31.154.151.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
31.154.151.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
79.181.134.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
84.110.34.148	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
84.108.133.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
87.68.249.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
168.235.207.129	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
46.121.87.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
190.189.249.156	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
77.125.76.164	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
79.176.131.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.67.37.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
213.57.139.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.66.53.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
190.189.249.156	Argentina	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
213.57.139.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.206.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.206.90	Block	956
149.78.206.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 149.78.206.90	Block	588
79.182.134.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	484
85.65.55.134	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.55.134	Block	406
84.229.167.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	365
79.182.134.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	292
85.65.55.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	291
77.126.68.43	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.68.43	Block	214
46.121.25.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	191
84.229.167.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	155
176.13.9.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
77.125.103.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
46.121.25.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
77.125.103.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	138
99.237.83.191	Canada	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 99.237.83.191	Block	136
79.179.26.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
176.13.9.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
77.126.68.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
46.19.86.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
149.78.206.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
84.229.167.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
79.182.134.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	97
77.125.6.255	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	92
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
37.142.68.68	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.68.68	Block	83
31.210.186.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
87.69.151.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
77.125.103.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	74
87.69.151.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
176.12.138.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
85.65.55.134	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.65.55.134	Block	65
176.13.17.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
207.241.226.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	57
46.19.86.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
46.121.25.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	55
176.13.9.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	51
109.160.254.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
149.88.136.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.118	Block	37
46.117.83.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
149.78.72.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.19.86.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
79.179.26.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
68.64.161.3	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.64.161.3	Block	31
131.253.25.243	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.186.90.116	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.90.116	Block	28