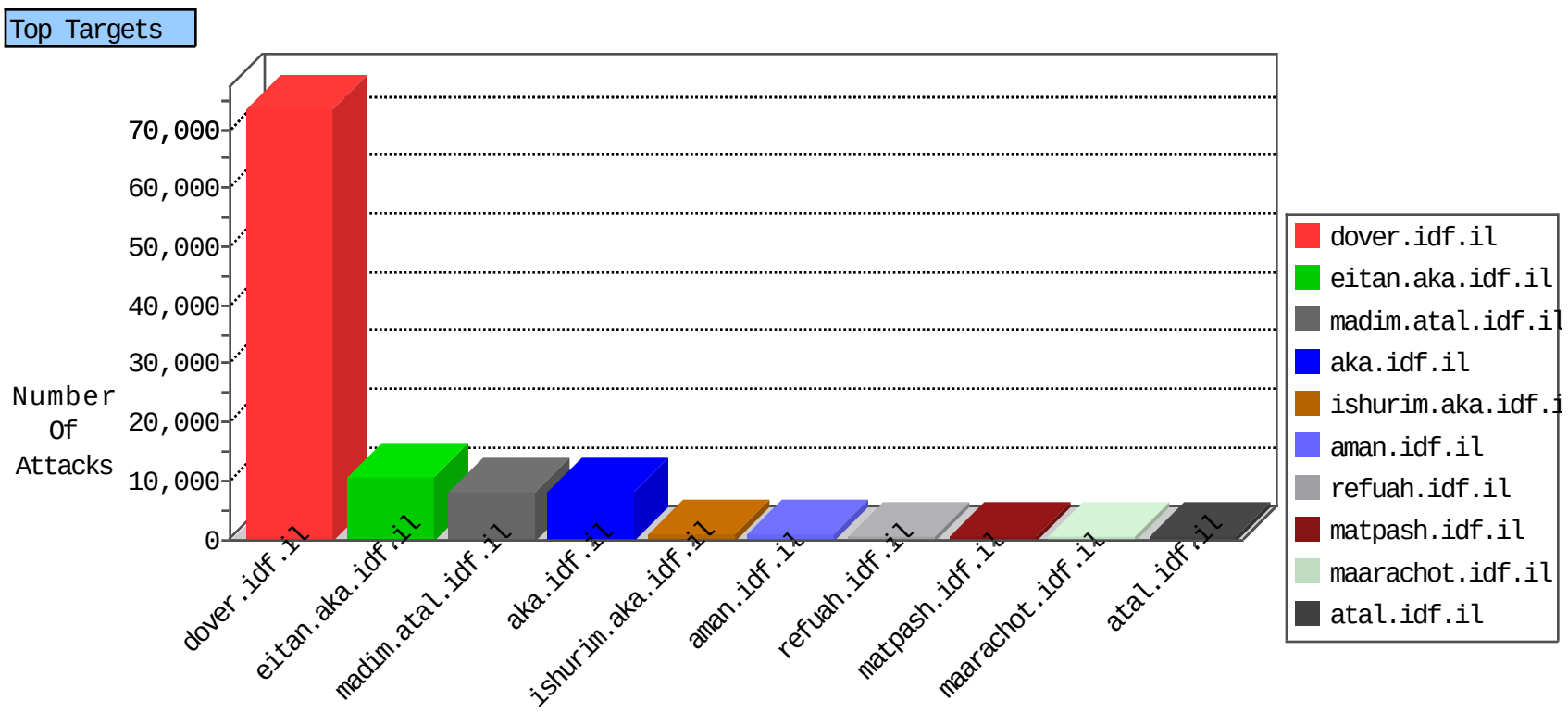
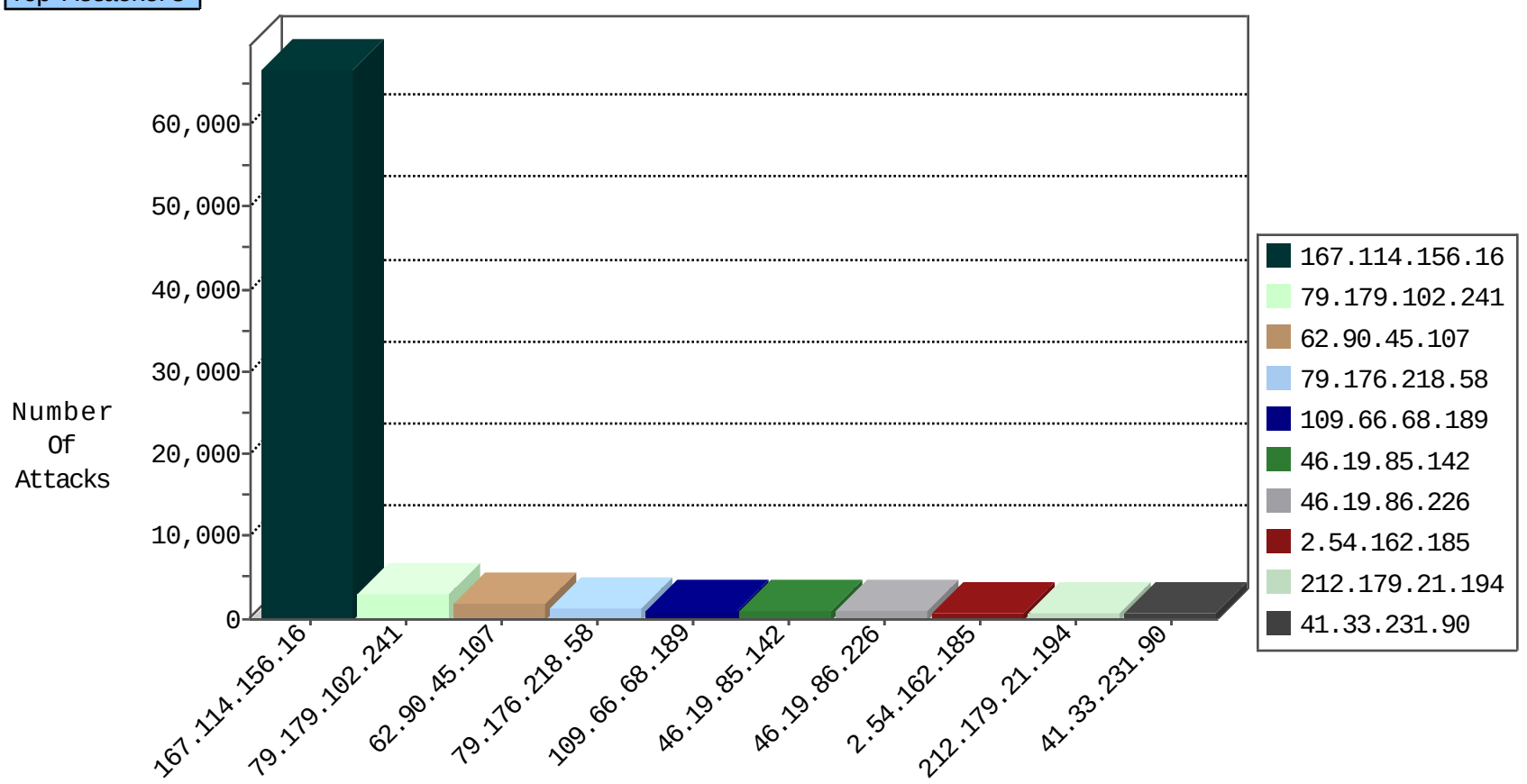
12-02-2015 to 12-03-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-02-2015 to 12-03-2015

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	90650
141.255.153.159	Netherlands	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	12672
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3695
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3557
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1293
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	647
66.249.66.111	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	488
66.249.66.1	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	376
66.249.93.198	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	356
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
37.26.148.174	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	102
66.249.64.153	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	94
66.249.66.78	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	72
66.249.66.5	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	23
79.183.14.170	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.179.221.157	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.180.134.148	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.178.108.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
75.104.23.170	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	5
79.181.206.157	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.7	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.179.196.188	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.65.215.149	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
93.174.93.151	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	3
31.168.170.222	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
46.19.85.96	Israel	147.237.77.233	atal.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
146.185.57.7	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
14.121.178.196	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.231.222.40	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
93.174.93.151	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
74.143.58.3	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.8	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
93.174.93.151	Netherlands	147.237.76.202	e.halag.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
203.87.112.185	Australia	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
93.174.93.151	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
123.182.243.196	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.25.51.226	Lithuania	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.76	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
120.132.77.184	China	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
202.112.51.96	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
192.3.170.124	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
103.224.22.13	Hong Kong	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-02-2015 to 12-03-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.193.34	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
64.251.25.176	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
184.168.193.34	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
24.47.146.194	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
63.143.34.37	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
89.19.29.90	Turkey	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
64.251.25.176	United States	147.237.76.42	refuah.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	8
158.85.253.245	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
189.38.90.212	Brazil	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
24.47.146.194	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
63.143.34.37	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
184.168.193.34	United States	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	5
91.142.253.133	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
195.154.211.20	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.191.162	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.188.74	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.194.47	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.188.186	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
151.80.31.129	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
80.212.19.243	Norway	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.180.24	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
185.106.94.2		147.237.77.170	maarachot.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
167.114.229.242	Canada	147.237.76.200	eitan.aka.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
91.142.253.133	Netherlands	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
188.165.15.138	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
184.168.193.34	United States	147.237.0.34	tikshuv.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
195.154.211.94	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
151.80.31.135	Italy	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.28	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
62.210.152.87	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.106.94.2		147.237.77.176	matpash.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
167.114.229.245	Canada	147.237.77.176	matpash.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
198.20.69.74	United States	147.237.77.227	e.hamaz.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
195.154.191.213	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
91.194.84.106	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.152	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.211.140	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
91.121.169.194	France	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
62.210.226.9	France	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
188.165.15.55	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
178.162.216.36	Germany	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
188.165.15.162	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
5.9.138.211	Germany	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.217.123	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
91.121.221.15	France	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.226.9	France	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

12-02-2015 to 12-03-2015

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	73
64.251.25.176	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	72
184.168.193.34	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	47
24.47.146.194	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	26
63.143.34.37	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	24
63.143.34.37	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	23
189.38.90.212	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	21
54.224.149.230	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	18
89.19.29.90	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	18
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	11
184.168.193.34	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	10
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	9
91.142.253.133	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	7
62.210.226.9	147.237.77.216	France	dover.idf.il	SQL Injection - Select From	6
212.179.159.253	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.79.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.79.3	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
171.232.56.152	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	4
85.165.60.202	147.237.0.33	Norway	idf.il	ET SCAN Potential SSH Scan	3
66.249.78.120	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	3
171.232.56.152	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
176.13.15.194	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
61.216.2.13	147.237.76.39	Taiwan	mobile.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
122.231.3.92	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	2
117.39.6.73	147.237.76.200	China	eitan.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.66.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	2
195.154.217.123	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	2
94.102.48.195	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.5	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.17.245	147.237.76.42	Israel	refuah.idf.il	GPL SCAN myscan	2
66.249.93.246	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
195.154.188.186	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
66.249.66.75	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.154.217.123	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
122.231.3.92	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.31	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
79.182.196.197	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
195.154.217.123	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypas Attempt (asp)	2
66.249.65.122	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
176.13.17.245	147.237.76.42	Israel	refuah.idf.il	INDICATOR-SCAN myscan	2
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
94.102.48.195	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.201	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.169.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.24.76.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-02-2015 to 12-03-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.102.241	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2382
79.176.218.58	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1122
109.66.68.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	864
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	778
2.54.162.185	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	723
79.182.104.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	690
46.19.86.71	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	465
173.254.203.98	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	285
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	276
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	272
199.203.196.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	252
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	242
62.207.60.228	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	162
82.166.83.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
213.57.135.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	94
213.57.135.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	94
213.57.136.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	86
100.100.104.89		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
100.100.47.166		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	74
46.19.85.110	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	66
46.19.86.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
46.19.86.55	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	63
79.181.179.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	61
46.19.86.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	59
132.71.160.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	58
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	56
213.57.135.213	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	51
100.100.104.89		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	51
100.100.120.170		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	49
79.182.130.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
94.159.141.180	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
84.108.128.246	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
46.19.86.92	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	46
132.71.170.7	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
213.57.135.213	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
46.19.86.119	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	44
109.66.124.221	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
100.100.107.247		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
46.19.86.46	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	36
79.176.14.147	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
100.100.90.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	36
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
108.54.59.192	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
46.244.85.192	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	35
100.100.78.10		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34

12-02-2015 to 12-03-2015

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.90.45.107	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.90.45.107	Block	1861
79.179.102.241	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	684
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	615
132.71.160.220	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	587
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.226	Block	547
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	427
193.106.55.244	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	399
176.13.15.194	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.15.194	Block	395
176.13.21.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	314
176.13.11.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	307
176.13.21.166	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.21.166	Block	296
80.246.136.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	267
109.66.104.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.66.104.45	Block	248
82.166.93.193	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	225
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	220
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	204
80.246.136.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	204
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	190
2.52.152.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	179
109.66.68.189	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.68.189	Block	177
176.13.15.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	174
80.246.136.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	173
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.226	Block	171
176.13.21.166	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.21.166	Block	163
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	161
132.71.170.7	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	158
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	155
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	149
2.52.152.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
109.66.104.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	129
199.203.196.245	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	123
207.241.226.42	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	122
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.95	Block	113
2.54.170.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
176.13.11.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
84.109.132.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
2.54.162.185	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
176.13.11.6	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.11.6	Block	97
185.32.179.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
79.182.104.177	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	88
193.106.54.36	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
176.13.15.194	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.15.194	Block	83
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.14	Block	81
84.109.132.61	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.109.132.61	Block	81
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	72
2.52.152.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	70
176.12.148.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
193.106.206.10	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58

12-02-2015 to 12-03-2015