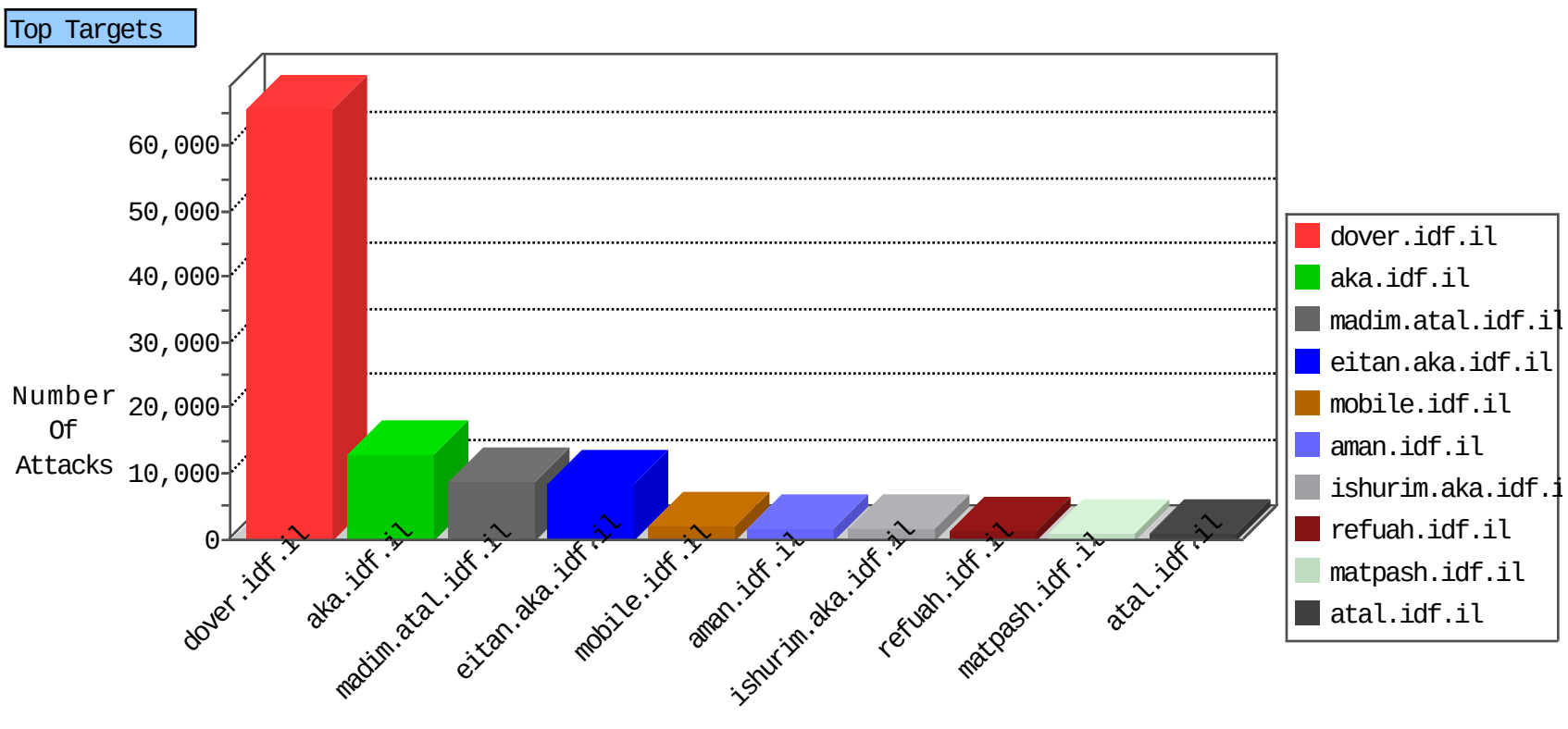
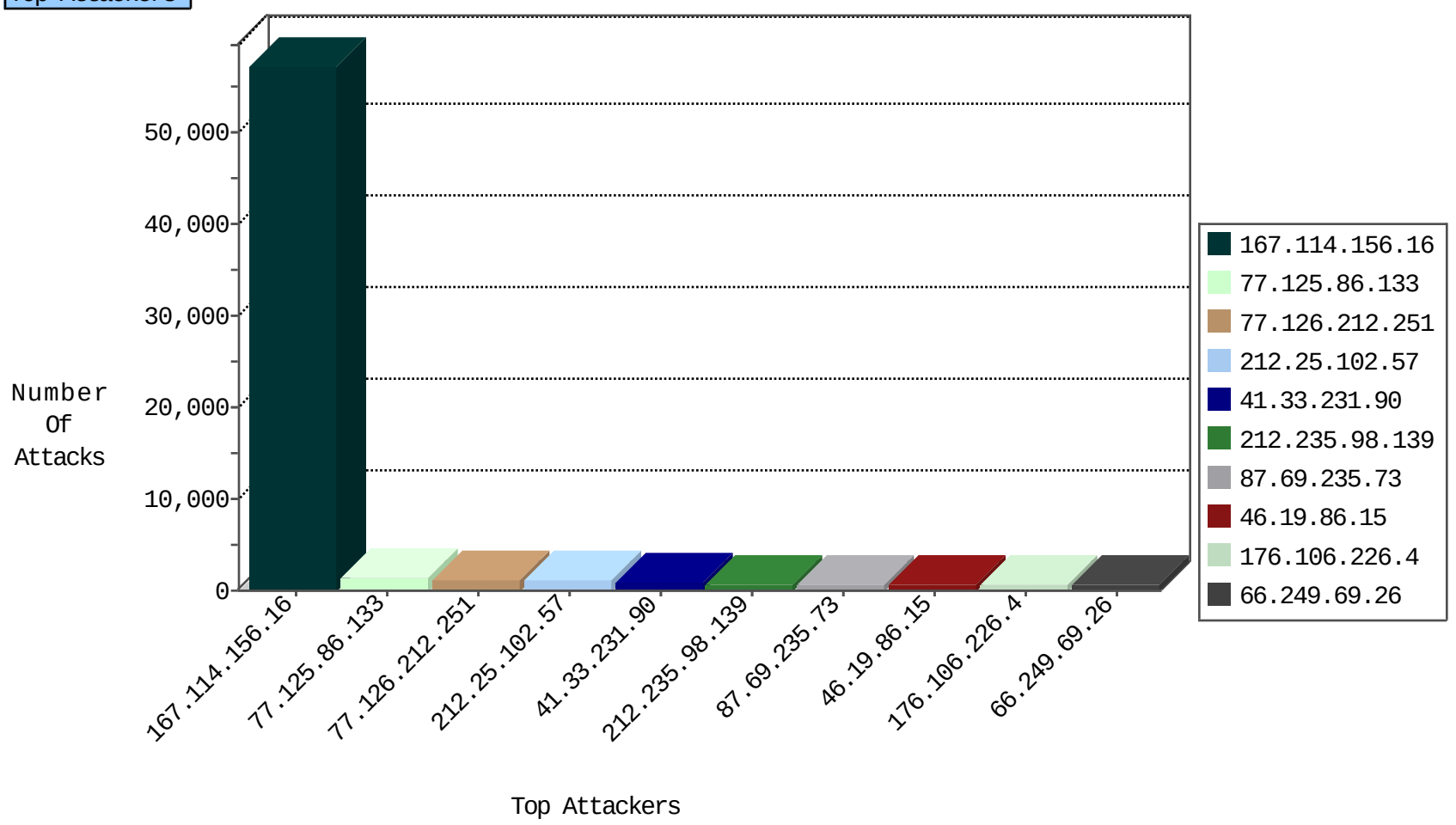
11-29-2015 to 11-30-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-29-2015 to 11-30-2015

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	90435
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	28905
66.249.67.243	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5084
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	943
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	877
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	749
91.231.193.150	Israel	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Http	drop	650
91.231.193.150	Israel	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	595
220.181.108.83	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	400
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	374
220.181.108.163	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	373
220.181.108.104	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	355
66.249.79.10	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	160
66.249.66.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	148
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
66.249.66.125	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	43
168.235.197.238	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	35
168.235.197.212	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	29
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
66.249.81.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
64.233.172.155	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
212.143.79.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
176.13.11.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
37.26.148.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
79.176.205.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.66.143.215	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.181.254.23	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
207.46.13.137	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.183.14.170	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
79.179.213.157	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
199.30.25.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
66.249.69.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
115.231.222.40	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	4
79.180.154.179	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	4
2.54.27.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
93.174.93.151	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	3
79.180.53.252	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
141.0.14.130	Europe	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	3
79.181.135.50	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
14.209.53.113	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	3
168.235.197.212	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Http	drop	3
79.180.134.246	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
66.220.146.30	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.105.235	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3

11-29-2015 to 11-30-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
118.238.227.101	Japan	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
67.216.79.204	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	14
109.186.160.125	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
87.242.112.35	Russian Federation	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
74.84.136.105	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
93.63.188.181	Italy	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
67.216.79.204	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
93.63.188.181	Italy	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.179.60.10	United Kingdom	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	7
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	7
81.218.97.114	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
31.154.10.131	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
87.242.112.36	Russian Federation	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	5
222.84.1.212	China	147.237.76.147	chinuch.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
212.25.95.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
195.154.216.86	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	4
212.199.54.130	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
213.8.125.176	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
194.54.168.76	Israel	147.237.77.233	atal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
195.62.18.126	Israel	147.237.76.86	navy.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
146.216.2.65	Switzerland	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
195.154.180.22	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	3
195.154.215.76	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.211.150	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.189.150	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.211.212	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
2.54.155.181	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.191.162	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.216.123	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
77.127.144.47	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.211.220	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
195.154.191.177	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
59.58.107.199	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
217.132.81.29	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.165.15.193	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	2
5.29.96.95	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.191.213	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
62.0.16.54	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
151.80.31.116	Italy	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.224	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.180.24	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
207.232.21.105	Israel	147.237.72.166	aka.idf.il	0495: HTTP: Shell Command Execution (cmd.exe)	Block	1
188.165.15.200	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
5.102.234.160	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
195.154.194.58	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.19	France	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.74	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.217.38	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-29-2015 to 11-30-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
67.216.79.204	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	69
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	66
118.238.227.101	147.237.77.74	Japan	law.idf.il	SQL Injection - Select From	24
192.198.151.43	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	22
93.63.188.181	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	19
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	17
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	13
87.242.112.35	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	13
176.13.5.214	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	9
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	5
87.242.112.36	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	5
66.249.75.247	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.254	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	3
195.154.191.177	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	3
195.154.215.76	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	3
195.154.217.38	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	3
195.154.217.38	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	3
195.154.216.123	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	3
195.154.217.38	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	3
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
192.198.151.45	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.154.211.150	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.154.211.150	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	2
176.13.4.223	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
206.162.239.75	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	2
195.154.180.22	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
195.154.216.86	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
185.120.126.34	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	2
198.20.69.74	147.237.77.179	United States	e.mazi.idf.il	ET DROP Dshield Block Listed Source	2
195.154.180.22	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
119.164.254.57	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
95.27.168.226	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
195.154.180.22	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	2
195.154.189.150	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
66.249.74.95	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.154.211.212	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
195.154.189.150	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS .asp Filename Extension Parsing File Upload Security Bypass Attempt (asp)	2
95.27.168.226	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
195.154.211.212	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.154.211.150	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
176.13.9.247	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
66.249.66.65	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
207.225.131.141	147.237.77.216	United States	dover.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
195.154.211.150	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
195.154.216.86	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
188.106.254.205	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	2

11-29-2015 to 11-30-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.86.133	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1236
77.126.212.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1038
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	785
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	568
176.106.226.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	567
82.81.19.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	486
5.102.219.215	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	453
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	450
46.19.85.98	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	429
77.125.141.51	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	360
37.26.146.131	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	351
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	307
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	279
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	184
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	118
46.19.86.98	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	110
46.19.85.79	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	109
81.218.135.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
141.0.14.130	Europe	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	99
141.0.14.130	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	90
213.57.134.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	89
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	87
168.235.197.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	86
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
37.19.119.184	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	81
37.142.196.252	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	77
109.64.171.235	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
100.100.84.58		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	75
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	73
213.57.128.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
213.57.128.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	69
100.100.33.74		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	69
46.19.86.13	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	68
46.19.86.78	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	67
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.19.86.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
109.67.206.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
100.100.62.204		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	60
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	57
46.19.86.15	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	57
212.150.214.90	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
85.250.60.23	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
46.19.86.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
80.178.202.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	52
100.100.76.150		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52

11-29-2015 to 11-30-2015

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
40.77.167.12	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1072
87.69.235.73	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.235.73	Block	346
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	301
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	219
87.69.235.73	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 87.69.235.73	Block	206
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	194
176.12.149.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	191
2.54.143.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	189
176.12.149.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
77.125.86.133	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	183
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	171
79.183.226.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	160
176.12.141.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	159
87.69.73.170	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.73.170	Block	157
77.126.212.251	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.212.251	Block	149
2.54.26.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
79.183.226.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
80.178.220.147	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
87.69.73.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
176.12.140.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
2.52.55.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	114
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
2.54.143.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.54.151.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
87.69.235.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.3.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	103
176.13.12.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
185.32.179.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
2.54.26.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
176.12.141.11	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	96
176.12.137.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
80.246.137.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
2.54.151.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	89
2.52.55.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	88
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.52.29.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
176.106.226.4	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 176.106.226.4	Block	83
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
176.13.7.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
212.199.101.60	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78