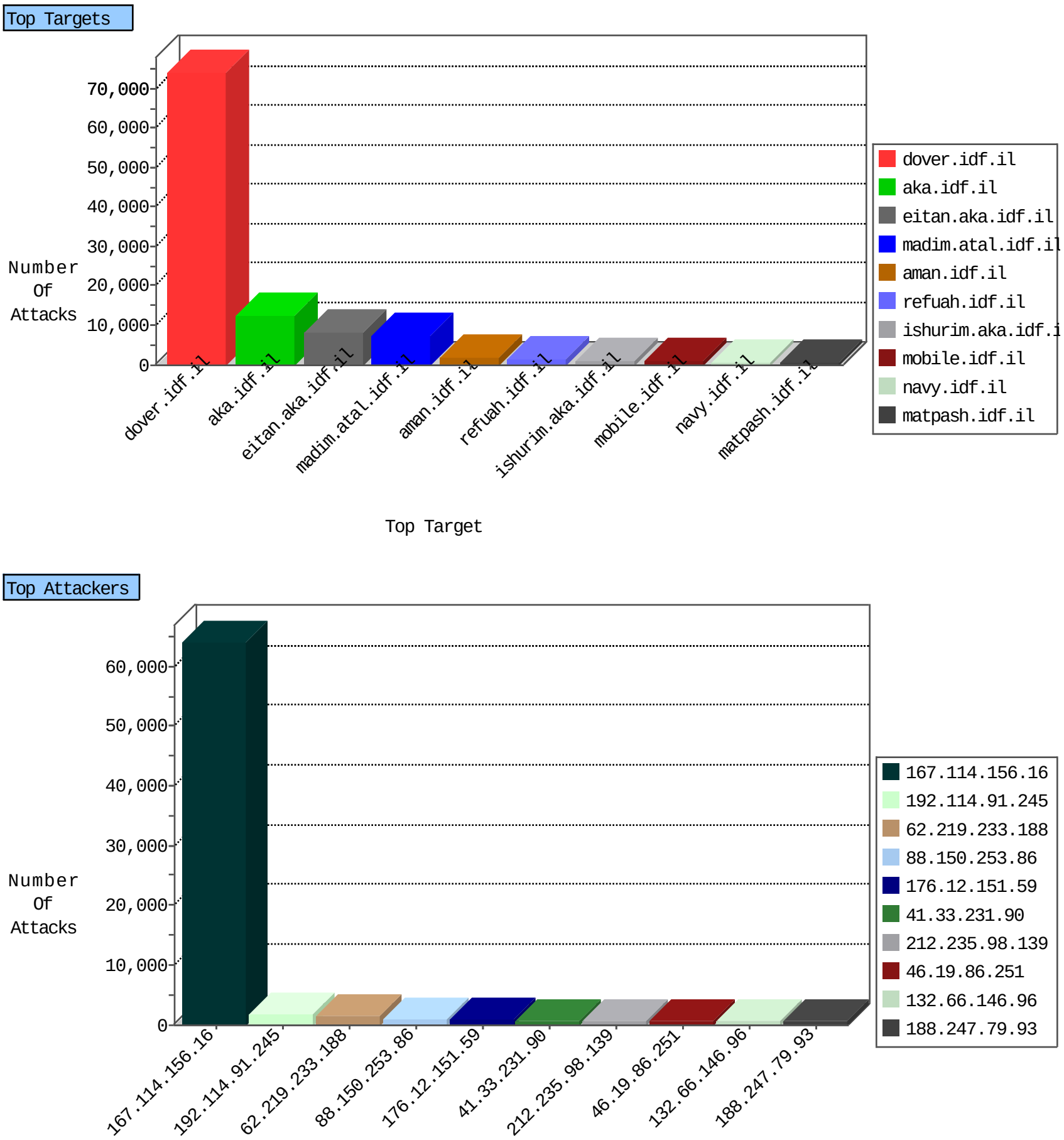
11-30-2015 to 12-01-2015

IDF Under Attack Daily Report



11-30-2015 to 12-01-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.108.92	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	412225
220.181.108.163	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	172542
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	90559
220.181.108.101	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	53690
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	17975
88.150.253.86	United Kingdom	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	9985
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1731
192.115.67.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	648
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	422
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	410
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	280
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	151
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	109
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
88.150.253.86	United Kingdom	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	42
88.150.253.86	United Kingdom	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	40
46.116.206.195	Israel	147.237.72.166	aka.idf.il	L4 Source or Dest Port Zero	drop	39
88.150.253.86	United Kingdom	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	35
88.150.253.86	United Kingdom	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	34
88.150.253.86	United Kingdom	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	32
88.150.253.86	United Kingdom	147.237.76.34	yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	26
88.150.253.86	United Kingdom	147.237.76.44	e.refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	26
88.150.253.86	United Kingdom	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	26
88.150.253.86	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	24
88.150.253.86	United Kingdom	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	24
88.150.253.86	United Kingdom	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	23
88.150.253.86	United Kingdom	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	22
88.150.253.86	United Kingdom	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	21
88.150.253.86	United Kingdom	147.237.76.31	nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	20
88.150.253.86	United Kingdom	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	19
88.150.253.86	United Kingdom	147.237.76.147	chinuch.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	17
88.150.253.86	United Kingdom	147.237.76.38	e.e.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	17
88.150.253.86	United Kingdom	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	17
88.150.253.86	United Kingdom	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	16
79.181.254.23	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
82.145.218.169	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
158.169.150.8	Belgium	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7
79.180.203.10	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
79.178.108.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
80.246.136.44	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
109.65.151.184	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
182.54.236.248	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.176.21.114	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
115.236.20.36	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	5
2.54.53.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5

11-30-2015 to 12-01-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.182.118.245	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.228.42.101	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
194.90.66.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
94.245.88.217	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.121.142.11	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	4
195.154.194.47	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	3
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	3
192.115.90.42	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
149.78.135.192	Israel	147.237.77.234	halag.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.25.95.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
46.116.239.84	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
115.236.20.36	China	147.237.76.39	mobile.meitav.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
188.165.15.32	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.211.30	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.158	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
94.245.88.135	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
188.165.15.239	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.217.216	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
151.80.31.128	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
109.226.18.234	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
195.154.180.22	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
85.64.38.129	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
216.170.119.193	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
195.154.211.212	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.188.186	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
178.63.13.15	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.76.199	e.nakchal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
111.206.116.217	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
195.154.194.58	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.28	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
85.89.73.242	Sweden	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.165.15.127	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.120.170.50	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
195.154.216.164	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
144.76.44.138	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
95.86.116.24	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
195.154.188.224	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
77.126.225.170	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
192.118.12.102	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
178.209.120.50	Russian Federation	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
198.20.69.74	United States	147.237.77.227	e.hamaz.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
195.154.194.59	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.35	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-30-2015 to 12-01-2015

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	72
79.180.3.42	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	42
46.19.85.45	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	17
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	13
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	9
94.245.88.217	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	6
66.249.66.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
195.154.189.150	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	3
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)	3
195.154.191.213	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	3
195.154.191.213	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
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
195.154.189.150	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	3
88.150.253.86	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	3
88.150.253.86	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	3
195.154.191.213	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	3
88.150.253.86	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
82.80.198.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
195.154.191.177	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
88.150.253.86	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.66.191.107	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
192.114.105.254	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
109.64.213.176	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	2
88.150.253.86	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
195.154.188.224	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
88.150.253.86	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
195.154.188.188	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
31.6.71.154	147.237.8.50	Poland	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
176.13.22.93	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
195.154.191.213	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP phptest.php access	2
66.249.73.221	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
88.150.253.86	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	2
88.150.253.86	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
88.150.253.86	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	2
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.66.5	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
14.142.33.102	147.237.0.16	India	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
195.154.189.150	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.154.188.224	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
208.90.155.46	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
195.154.188.224	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
66.249.81.198	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
176.13.22.93	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
195.154.194.47	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
31.6.71.154	147.237.0.35	Poland	akaws.idf.il	ET SCAN NMAP -sS window 1024	2

11-30-2015 to 12-01-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.114.91.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1371
62.219.233.188	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1146
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	759
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	715
132.66.146.96	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	576
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	540
80.246.133.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	533
2.52.36.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	471
79.177.123.198	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	462
37.26.148.152	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	462
2.54.28.91	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	317
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	236
37.153.253.106	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
213.57.137.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	233
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	210
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	190
62.219.124.98	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	184
199.203.215.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	144
199.203.215.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	144
192.176.65.1	Sweden	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	130
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
5.102.234.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	126
79.177.212.31	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
89.138.12.90	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	112
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	112
2.54.177.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	108
80.246.133.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	105
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	99
46.19.86.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	93
89.237.149.237	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	92
213.57.133.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	89
84.111.36.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
84.108.137.200	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	84
188.247.79.93	Jordan	147.237.77.216	dover.idf.il	drop		drop	76
213.57.133.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	72
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
192.115.67.2	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	70
212.199.244.112	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	67
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
217.194.196.207	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	58
213.57.131.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
213.57.136.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
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
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
213.57.136.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	53
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
85.65.235.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.151.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	504
95.86.78.46	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	460
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.251	Block	406
192.114.91.245	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	345
46.116.121.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	341
2.52.182.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	301
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	284
62.219.233.188	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	253
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.34	Block	243
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	227
176.12.151.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	218
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	191
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	191
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.3.125	Block	181
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	177
176.12.141.174	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.141.174	Block	170
84.111.36.204	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	169
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
176.12.142.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
212.76.105.35	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	149
46.116.121.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
176.12.151.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	141
2.52.182.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	137
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.251	Block	122
2.54.3.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
2.54.181.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
176.12.141.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.52.182.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
2.54.25.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
197.131.8.56	Morocco	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	101
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	96
2.54.25.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.25.136	Block	95
176.13.11.87	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
46.116.121.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	88
132.66.146.96	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
109.253.43.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
37.142.68.105	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	67
207.241.226.41	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	65
80.246.130.205	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
176.12.142.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	62