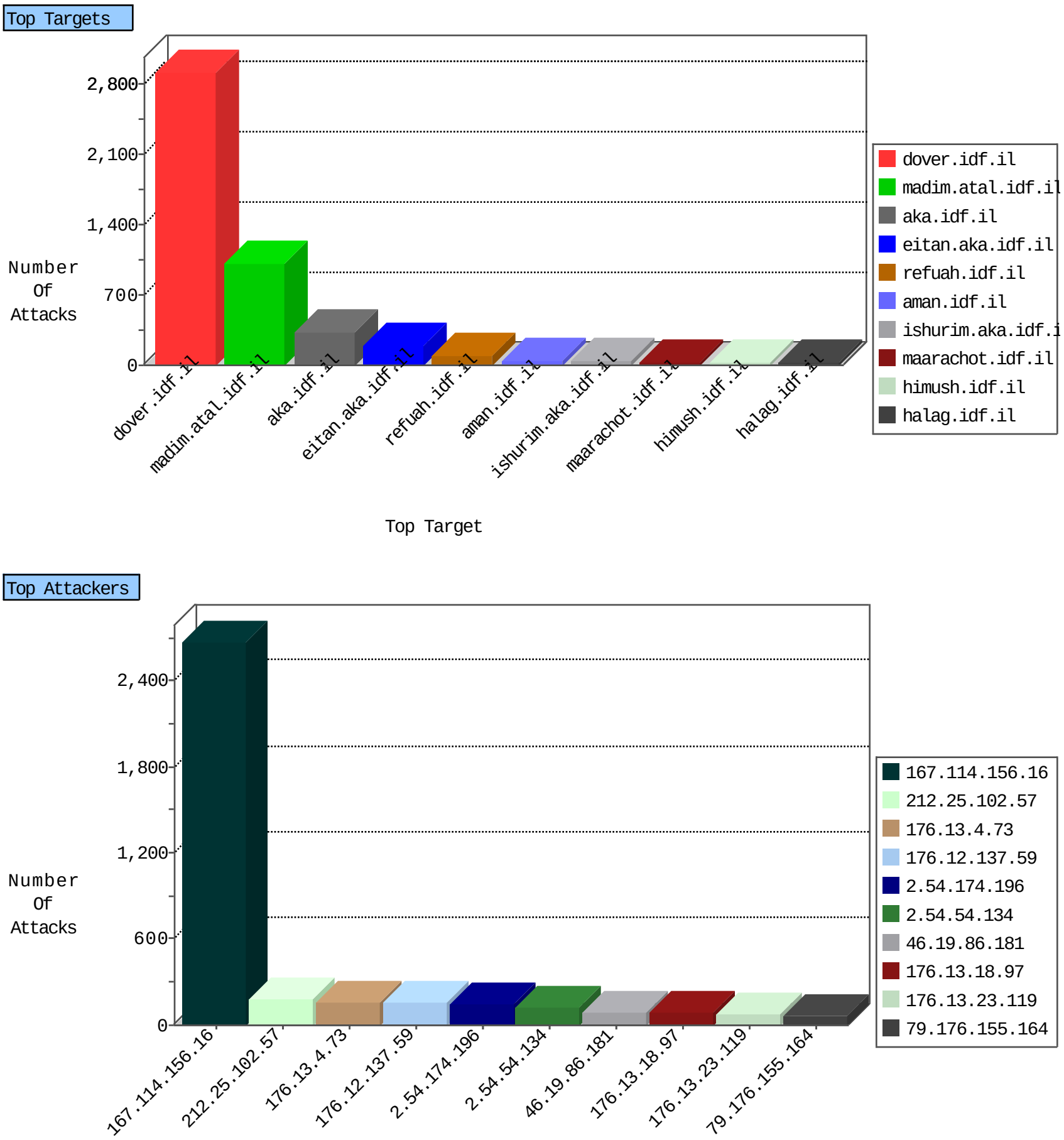
12-10-2015-17:04:05 to 12-10-2015-18:04:05

IDF Under Attack Daily Report



12-10-2015-17:04:05 to 12-10-2015-18:04:05

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	3446
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	56
109.67.113.97	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	34
2.54.16.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.57.182.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
158.69.199.64	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
158.69.199.64	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-10-2015-17:04:05 to 12-10-2015-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.106.94.2		147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.106.94.2		147.237.72.156	aman.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
52.35.180.120	United States	147.237.76.42	refuah.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
52.35.187.114	United States	147.237.72.166	aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
186.213.19.210	Brazil	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
112.111.188.201	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
185.106.94.2		147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

12-10-2015-17:04:05 to 12-10-2015-18:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	3
66.249.65.9	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
158.255.2.52	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.58.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.130.68	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
84.110.53.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.205.52.4	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.177.21.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.205.52.4	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.117.204.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.85.31.170	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.102.254.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.40.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.2	147.237.0.17		m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
158.255.2.52	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
109.64.15.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.207.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.130.68	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
79.178.143.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.205.52.4	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
213.85.31.170	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.117.77.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.74.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-10-2015-17:04:05 to 12-10-2015-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.106.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
46.19.85.212	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.143.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
5.28.145.145	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
46.19.85.198	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
5.28.155.154	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
185.3.146.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
31.154.170.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.174.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
94.230.86.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.157.4	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
199.30.25.171	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.112	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.250.245.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.54.40.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.60.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
179.4.205.97	Chile	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.147.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.134.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.128.233	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
179.4.205.97	Chile	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
179.4.205.97	Chile	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.228.132.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.129.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
207.241.226.41	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
188.120.148.148	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
5.22.134.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.28.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.174.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.174.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.190.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.174.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
213.57.130.216	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.22.134.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.130.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.153.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.140.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.25.102.57	Israel	147.237.77.61	e.cogat.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
82.80.230.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-10-2015-17:04:05 to 12-10-2015-18:04:05

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	181
176.12.137.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
2.54.174.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	119
176.13.4.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
2.54.54.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
176.13.23.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.13.18.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
79.176.155.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
176.13.4.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.181	Block	33
80.246.136.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
2.54.54.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
176.13.18.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
2.54.174.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
85.64.181.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.115.99.130	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113005.pdf	Block	5
109.65.57.55	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	4
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	4
132.66.222.158	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 132.66.222.158 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	3
46.118.155.216	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
95.134.121.18	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/sip_storage/files/1/2461.jpg	Block	3
84.108.22.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.51	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.32.179.114	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
109.65.37.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.52.165.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
52.35.180.120	United States	147.237.76.42	refuah.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
176.13.16.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
62.219.92.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	2
185.3.146.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.177.148	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.179.177.148 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	2
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.38.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.49	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/common/logininfo.aspx	Block	1
94.230.86.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/kurs/default.asp	Block	1
52.35.187.114	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1
176.13.14.115	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding O_cJW&7[&%_Wb:}h{U&	None	1
77.126.147.181	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=0%7C45%2C0%7C46%2C1%7C47%2C0%7C48%2C1%7C49; __atuvs=56699e451f926573000; __atssc=facebook%3B7	Block	1
109.65.15.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-10-2015-17:04:05 to 12-10-2015-18:04:05