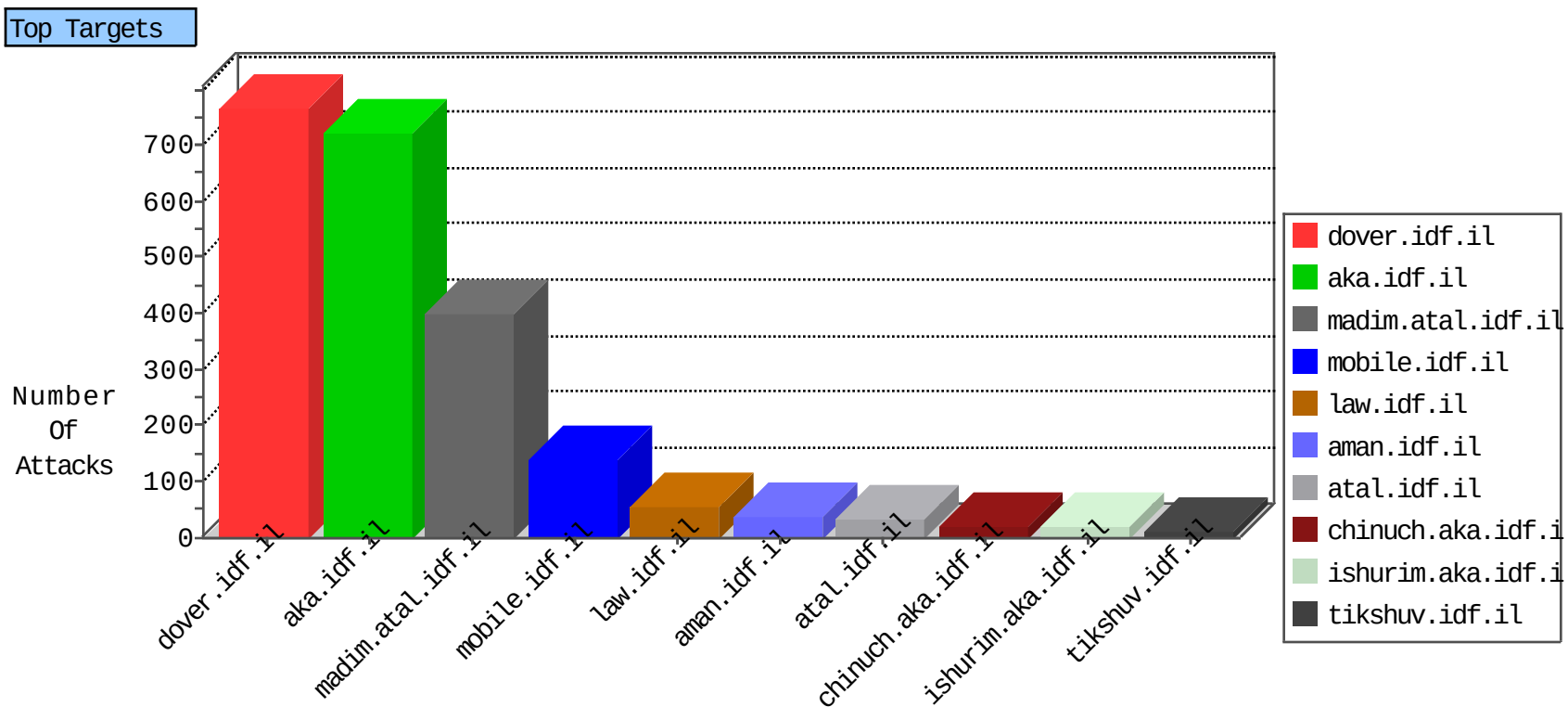
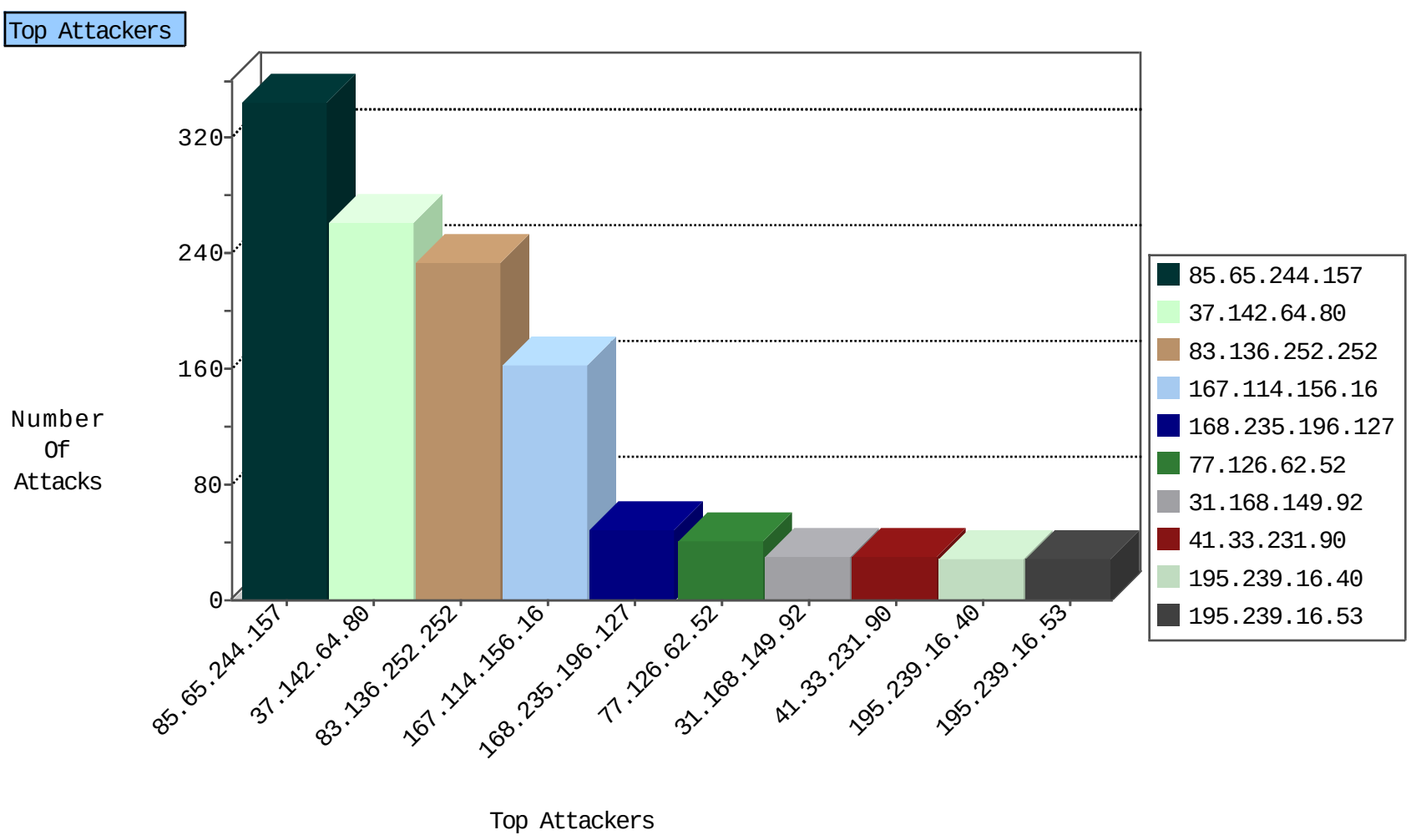
12-29-2015-23:04:07 to 12-30-2015-00:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-29-2015-23:04:07 to 12-30-2015-00:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.41.65	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	21396
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2437
176.228.192.105	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	895
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	145
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	136
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	32
212.150.126.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
173.252.74.99	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
79.176.28.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
185.120.125.30		147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5
181.160.213.42	Chile	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.176.100.246	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
79.182.20.77	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4
83.136.252.252	United Kingdom	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
181.160.213.42	Chile	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
222.186.42.20	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
176.13.4.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
157.55.39.227	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
168.235.196.127	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
107.21.1.8	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-29-2015-23:04:07 to 12-30-2015-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-29-2015-23:04:07 to 12-30-2015-00:04:07

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	4
66.249.78.166	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
168.62.238.153	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
151.217.178.80	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.176		test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.30.152	147.237.0.15		kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
118.68.29.67	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
191.33.22.198	147.237.77.205	Brazil	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
191.33.22.198	147.237.77.205	Brazil	prisha.idf.il	ET SCAN NMAP -f -sS	1
95.86.71.196	147.237.72.166	Israel	aka.idf.il	SERVER-WEBAPP apache directory disclosure attempt	1
182.212.149.19	147.237.76.38	Korea, Republic of	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.233.30.122	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.76.30		himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.29.136.96	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
151.217.178.80	147.237.8.14		e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.148		gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
208.67.1.155	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
119.81.60.162	147.237.76.38	Singapore	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
192.186.95.178	147.237.8.27	Canada	e.madim.atal.idf.i	ET SCAN NMAP -sS window 4096	1
118.68.29.67	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
191.33.22.198	147.237.77.205	Brazil	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.30.70.132	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.86.71.196	147.237.72.166	Israel	aka.idf.il	GPL WEB_SERVER apache directory disclosure attempt	1

12-29-2015-23:04:07 to 12-30-2015-00:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
83.136.252.252	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	229
168.235.196.127	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
85.65.244.157	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
77.127.227.190	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	26
79.183.201.110	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
109.253.192.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
77.126.62.52	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
31.168.149.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	19
109.65.35.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.94.74.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.85.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
213.8.204.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
213.8.204.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
94.159.230.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
181.160.213.42	Chile	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.108.8.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.12.150.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.176.100.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
89.139.154.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.174.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.136.219	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.199.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.141.181	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.179.155.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.141.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
104.217.216.173	United States	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	6
77.126.8.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.62.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.156.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.114.91.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.250.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
31.210.188.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
128.255.155.26	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.140.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.140.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
128.255.155.26	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.203	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.8.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.65.103.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

12-29-2015-23:04:07 to 12-30-2015-00:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.64.80	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.64.80	Block	261
85.65.244.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	162
85.65.244.157	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.244.157	Block	134
109.253.211.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
77.126.62.52	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.62.52	Block	20
109.65.164.19	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	11
2.52.135.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
213.8.204.50	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
85.65.244.157	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.65.244.157	Block	7
84.94.74.77	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
85.130.137.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
109.253.192.255	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.177.62.244	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
176.12.150.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
207.46.13.164	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
2.54.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.9.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.35.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.10.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.137.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.165.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.132.114.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	2
213.8.204.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.108.8.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.68.100	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.7.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.50.89.148	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.139.154.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.146.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.244.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.133.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.65.207.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.141.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
184.168.200.194	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
5.107.71.10	United Arab Emirates	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
93.173.237.191	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.13.1.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
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	1
31.154.145.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.15.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
85.250.253.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20422-he/idfgdover.aspx	Block	1
84.228.38.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl79 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.121.121.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.123.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-29-2015-23:04:07 to 12-30-2015-00:04:07