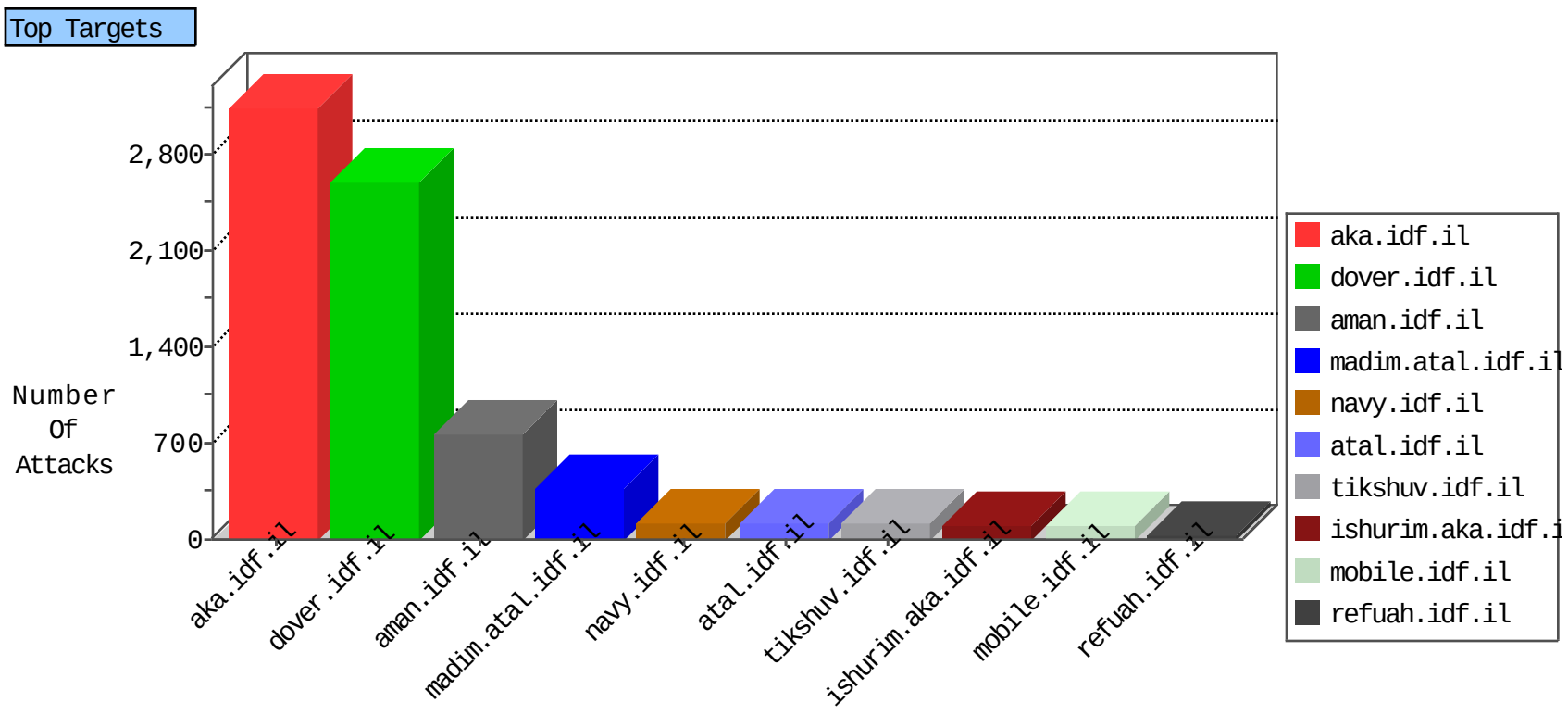
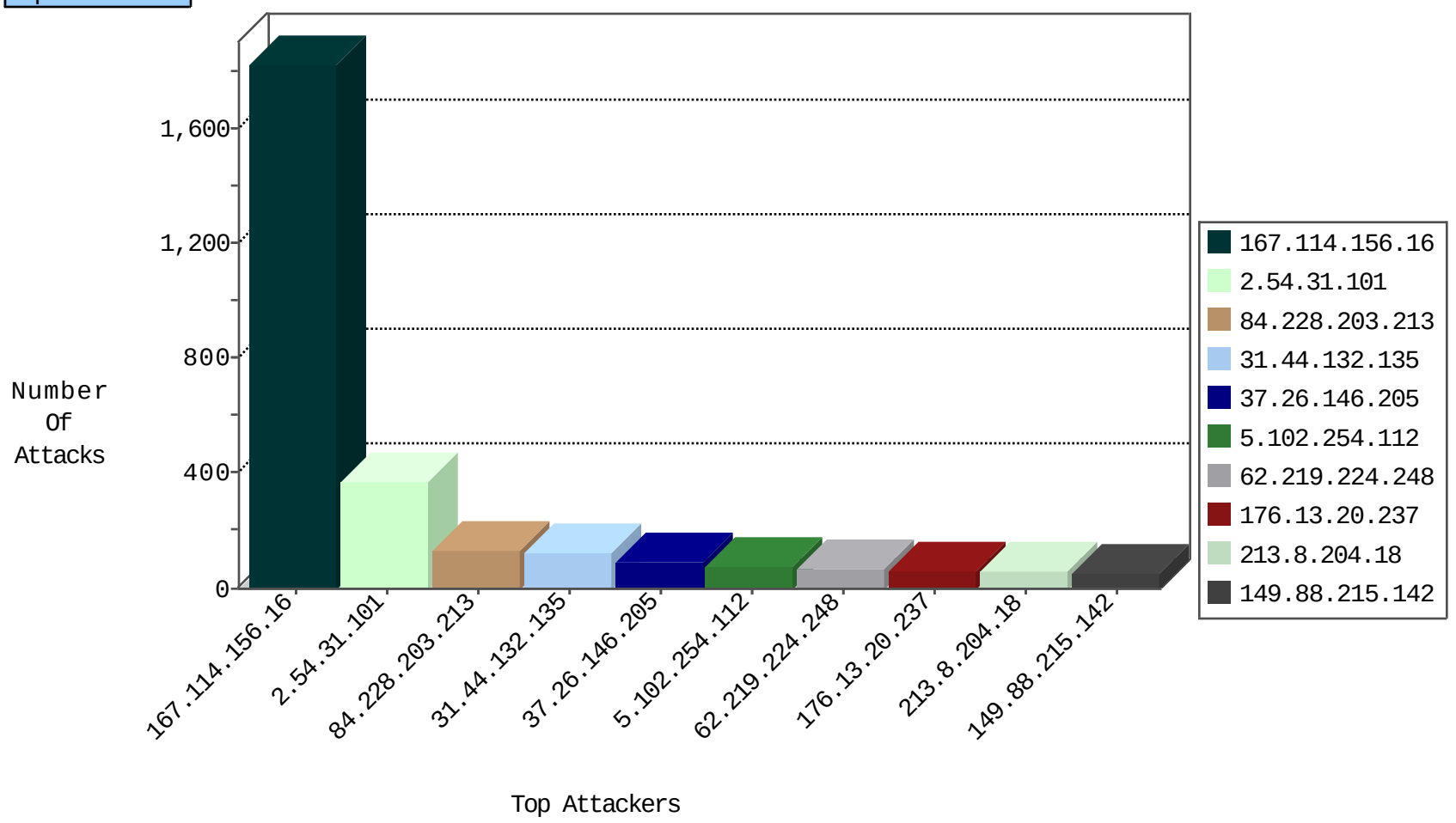
12-17-2015-16:04:01 to 12-17-2015-17:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-17-2015-16:04:01 to 12-17-2015-17:04:01

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	3143
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
168.235.197.254	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	50
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
168.235.197.254	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	2
93.174.93.181	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
93.158.203.169	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
61.182.170.38	China	147.237.76.31	nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
93.174.93.181	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
61.182.170.38	China	147.237.76.34	yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

12-17-2015-16:04:01 to 12-17-2015-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-17-2015-16:04:01 to 12-17-2015-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.58	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
36.72.228.72	147.237.72.166	Indonesia	aka.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
5.79.68.161	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.125.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.42.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.191.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
46.117.199.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.72.166	Indonesia	aka.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.72.166	Indonesia	aka.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
62.75.236.76	147.237.0.33	Germany	idf.il	ET SCAN NMAP -sS window 1024	1
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	1
46.19.85.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-17-2015-16:04:01 to 12-17-2015-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.205	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	95
31.44.132.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	63
31.44.132.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
5.102.254.112	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
84.228.203.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
84.228.203.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
168.235.197.254	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
84.228.203.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
2.54.41.78	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	26
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
207.241.229.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
84.228.203.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	25
176.13.20.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
79.176.191.56	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
62.219.224.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
62.219.224.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
185.3.144.84	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
149.88.215.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
79.183.178.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
62.219.224.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
2.54.180.237	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
5.29.205.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
5.29.205.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
149.88.215.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	18
46.19.86.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
176.13.2.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
176.13.20.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
46.19.86.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	17
2.54.180.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
79.183.116.232	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.86.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
80.246.136.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
109.253.136.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.54.180.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
84.109.39.134	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
31.168.72.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	15
37.142.137.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.102.254.112	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
176.13.20.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
31.168.92.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
176.13.15.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
147.236.232.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.223	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
213.8.204.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
176.13.15.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14

12-17-2015-16:04:01 to 12-17-2015-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.31.101	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.31.101	Block	193
2.54.31.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	155
176.13.10.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
221.178.182.156	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	7
221.178.182.131	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	6
103.252.17.160	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	5
221.178.182.176	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	5
103.252.17.160	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 103.252.17.160	Block	5
218.205.17.208	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	5
221.178.182.204	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/templates/sendtofriend/	Block	5
37.142.137.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.15.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.136.234	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
190.207.230.111	Venezuela	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/sendtofriend/	Block	3
218.205.17.164	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1155-he/navy.aspx#par_4	Block	3
84.228.64.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
37.142.68.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
186.95.194.64	Venezuela	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/templates/sendtofriend/	Block	3
79.182.107.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	2
221.178.182.207	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1155-he/navy.aspx#par_5	Block	2
221.178.182.140	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1156-he/navy.aspx#par_4	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
71.41.182.242	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1155-he/navy.aspx#par_1	Block	2
31.131.16.162	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.131.16.162	Block	2
45.79.169.195		147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	2
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	2
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.143.138.230	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/510-he/patzar.asph	Block	2
218.205.17.145	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/1155-he/navy.aspx#par_5	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
80.230.67.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
31.168.236.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	2
221.178.182.171	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/templates/sendtofriend/	Block	2
77.126.78.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
176.12.145.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.248.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
221.178.182.134	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/1155-he/navy.aspx#par_5	Block	1
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	1
66.249.66.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.206.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.57.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.116.203.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=1%7C49%2C1%7C50; __atuvs=5672c0bbf66b90da000	Block	1
85.64.53.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.191.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.142.64.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.131.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-17-2015-16:04:01 to 12-17-2015-17:04:01