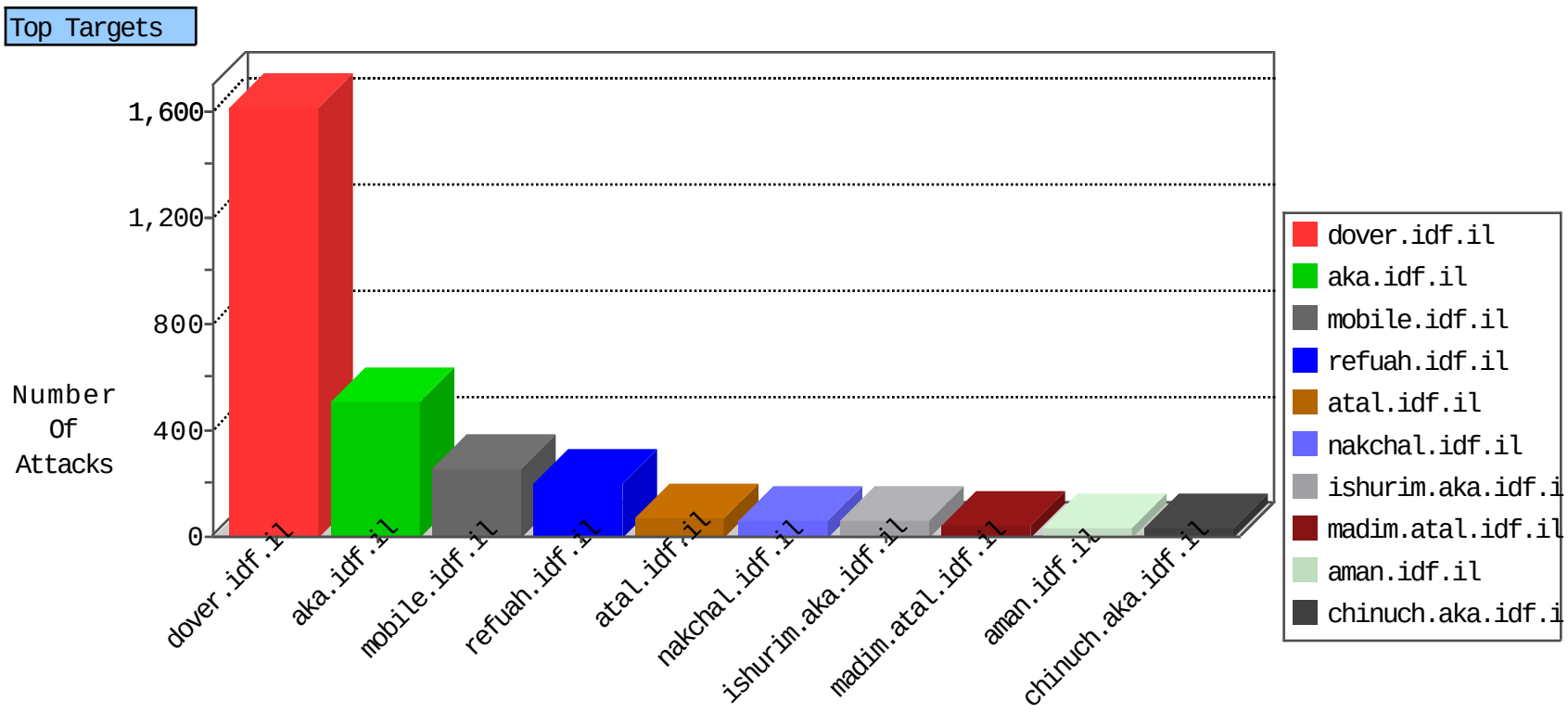
12-30-2015-16:04:00 to 12-30-2015-17:04:00

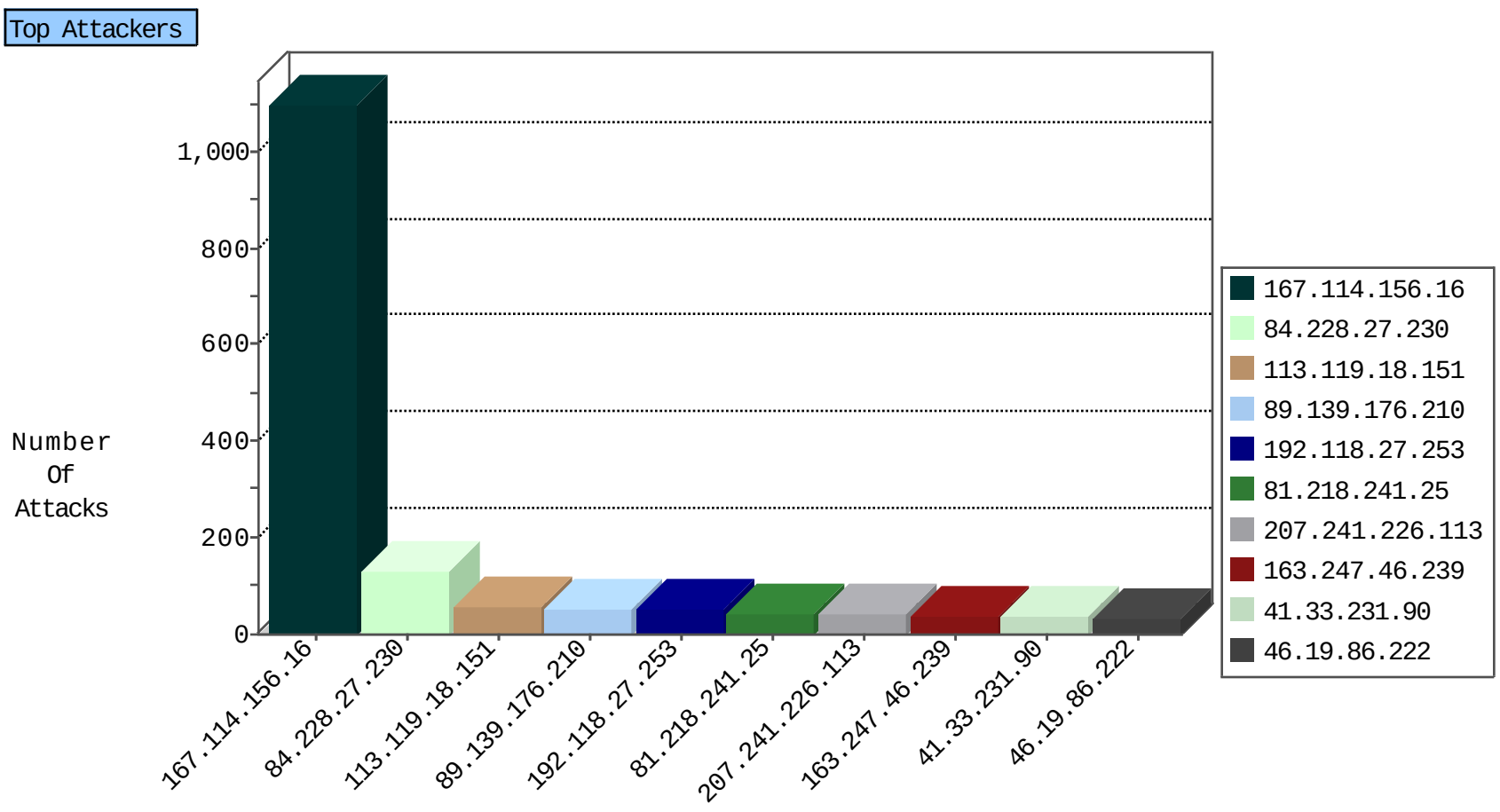
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-30-2015-16:04:00 to 12-30-2015-17:04:00

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	3128
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
81.23.86.124	Italy	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
94.102.56.238	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
106.75.199.192	China	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
109.253.138.39	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
94.102.56.238	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

12-30-2015-16:04:00 to 12-30-2015-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-30-2015-16:04:00 to 12-30-2015-17:04:00

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	2
207.241.226.113	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
132.71.121.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.11.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.0.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.13.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.72.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.181.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.153.104.125	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -f -sS	1
40.115.57.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.14.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.14.42	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
96.44.187.158	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.13.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.189.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.115.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.126.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.153.104.125	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
46.121.137.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.203.178.148	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.58.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.14.42	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1

12-30-2015-16:04:00 to 12-30-2015-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.228.27.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	129
89.139.176.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
207.241.226.113	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
163.247.46.239	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.86.222	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	34
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
113.119.18.151	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
37.26.147.199	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
80.246.136.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
188.161.63.158	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
46.19.86.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
176.13.9.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.165.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
80.178.157.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
79.182.56.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.171.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.54.13.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.214	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
85.65.57.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.249.65.135	Algeria	147.237.77.216	dover.idf.il	drop		drop	11
37.26.146.247	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	11
147.235.8.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
147.235.8.70	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.108.50.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.52.172.193	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
5.102.254.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
176.13.15.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.216	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.93.63.173	Ukraine	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
192.118.27.253	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.13.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.220	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
81.199.122.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
5.22.130.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.189.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.133.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

12-30-2015-16:04:00 to 12-30-2015-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.119.18.151	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.119.18.151	Block	27
176.13.18.18	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	17
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	13
77.93.63.173	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.93.63.173	Block	13
176.13.16.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
89.138.160.6	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
80.178.157.105	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.13.9.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
109.253.205.141	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	5
80.246.136.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.55	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.8.245.50	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.245.50	Block	3
46.19.86.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
85.64.1.174	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
109.253.213.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.109.127.9	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1598	Block	3
212.76.104.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	3
66.249.66.52	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.16.82	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.132	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
46.19.86.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.215	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.109.127.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.150.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.172.187.42	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.49.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.14.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.128.24	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
84.109.127.9	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.109.127.9	Block	2
109.253.198.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.238.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.133.51	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 109.64.171.89 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
113.119.18.151	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
185.32.179.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.205.23	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.56	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
176.13.19.103	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
213.151.35.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.1.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.103	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	2
46.19.85.37	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Ã±Ã Â©Ã½Ã£Y[[#31]][[#6]][7ÂŸÂ€[[#25]]ÂžÂ[[#0]][[#3]]Â¹Â²3NÃ–NÂ¦Â¼bÂ¢[[#25]]ÂºÃˆÃ‰Ã·Ã›"Ã¤Â¬wÂ§Â–Ã”Âœ(Ã®-#Â¿Â‡hÂšÃƒP[[#17]]4Â¡CÃ‹:Jab[[#4]]Â©Ã[[#17]]Â¦KÂ¡NiÃ®Â’E,Ã?Ã?F[[#3]]Â›yVÂŠpAC.lE1[[#15]][[#28]]Â [[#19]]Ã?Ã¶[[#22]][[#18]]wÂ?ÂŽÂ–Â ÃœÂ…Â·~[[#16]]ÂµÂ?Â“E#Â½Â©Ã?Â½Ã³Ã´Ã“SÂ©Â¢Ã‘Ã®sÃ™Ã–Â¸Ã™Â°)[[#8]][[#30]]Âº.2	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
37.26.146.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.50.179	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$atudaControl$firstAtudaControl$ctl00$Mossad in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
149.78.231.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-30-2015-16:04:00 to 12-30-2015-17:04:00