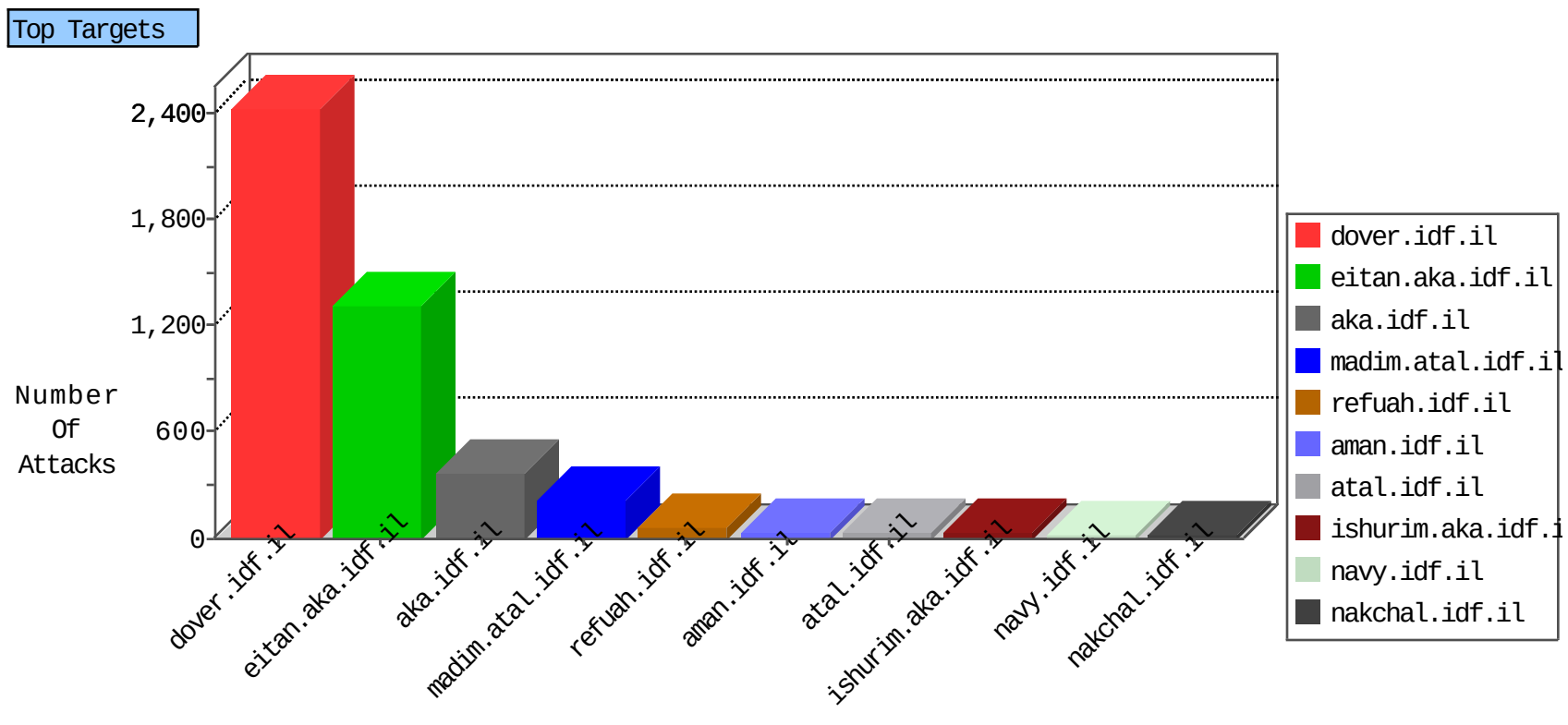
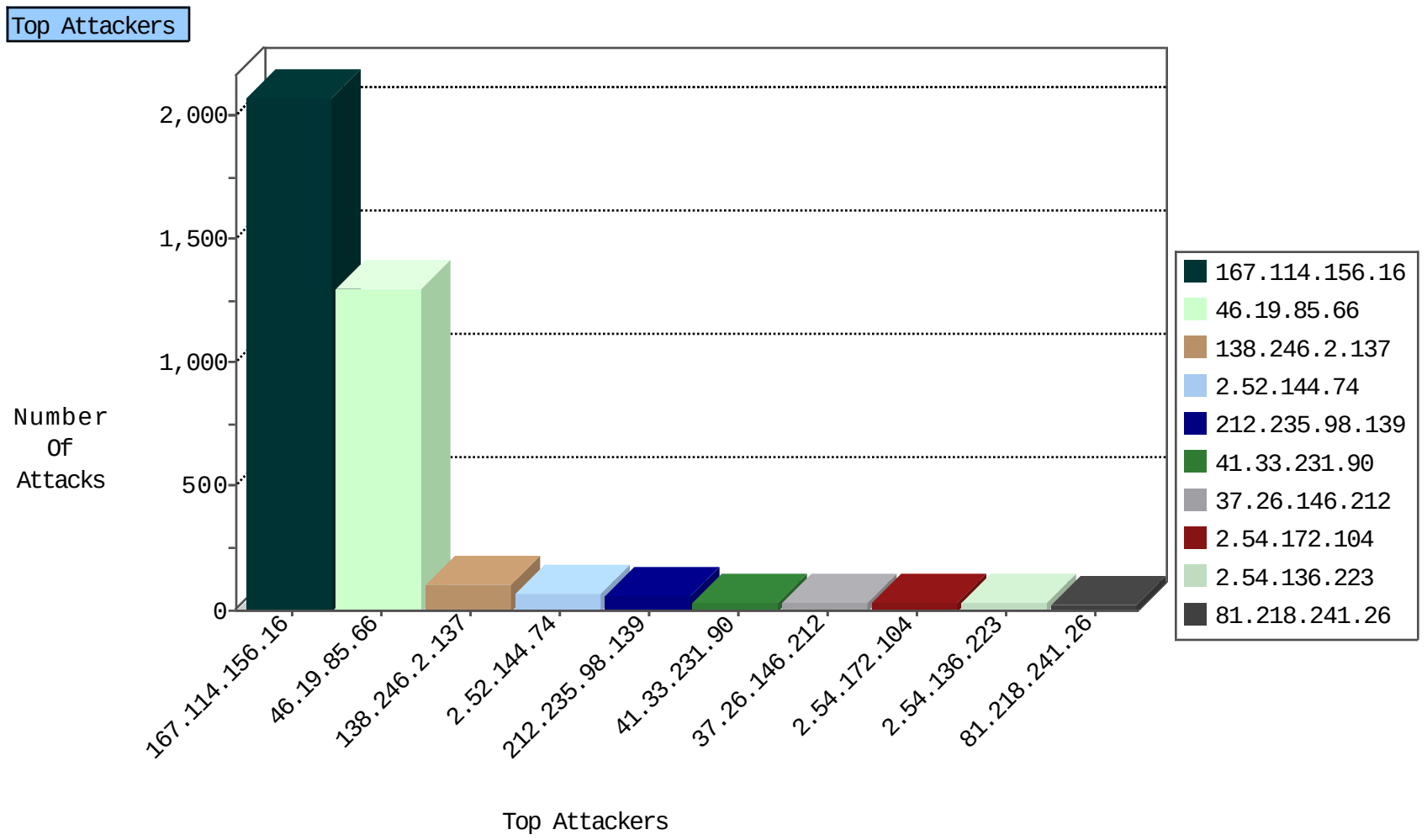
12-14-2015-16:04:01 to 12-14-2015-17:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-14-2015-16:04:01 to 12-14-2015-17:04:01

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	3238
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
80.82.64.198	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
1.195.8.250	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1

12-14-2015-16:04:01 to 12-14-2015-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.177.148	Israel	147.237.72.166	aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1

12-14-2015-16:04:01 to 12-14-2015-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.25.217.91	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.94.198.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.79.104	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
23.97.172.218	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
192.115.248.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
175.196.159.201	147.237.77.61	Korea, Republic of	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.78.150.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
85.25.217.91	147.237.77.233	Germany	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.25.217.91	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.180.68.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.90	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.89.217.234	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.230.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.150.29.211	147.237.8.46	Australia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.152.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-14-2015-16:04:01 to 12-14-2015-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1254
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
81.218.66.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
77.126.167.198	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.54.172.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
213.57.137.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.176.42.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.86.90	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.148.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.15.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
188.120.148.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.176.42.149	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.179.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.221.59.28	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
5.102.254.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.221.59.28	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
185.89.217.235		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
79.181.141.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
76.167.133.97	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.172.104	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	6
46.117.6.111	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.221.59.28	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
79.178.180.79	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.221.59.28	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.179.9.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.140.17	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
93.172.149.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.148.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.115.92.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.130.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.172.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
213.57.130.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.89.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
176.12.146.51	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.65.167.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.172.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

12-14-2015-16:04:01 to 12-14-2015-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.144.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
138.246.2.137	Germany	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 138.246.2.137	Block	53
138.246.2.137	Germany	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 138.246.2.137	Block	53
46.19.85.66	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.66	Block	51
37.26.146.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.136.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
37.26.146.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.12.151.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	5
212.179.180.30	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	4
213.8.204.74	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	3
149.78.243.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.12.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.74	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	3
91.183.174.34	Belgium	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	3
176.13.17.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.164.66	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
2.52.176.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
2.54.2.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.111.69	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
185.32.179.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.12.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.152.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.44.132.135	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
46.121.158.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.121.158.41	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.19.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.178.182.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.86.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.137.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.236.200.93	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
70.138.150.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 70.138.150.82	Block	1
5.28.190.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.190.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.64.75	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.42.149	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1405-he/refuah.aspx	Block	1
66.249.79.217	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
95.35.37.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.83.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-14-2015-16:04:01 to 12-14-2015-17:04:01