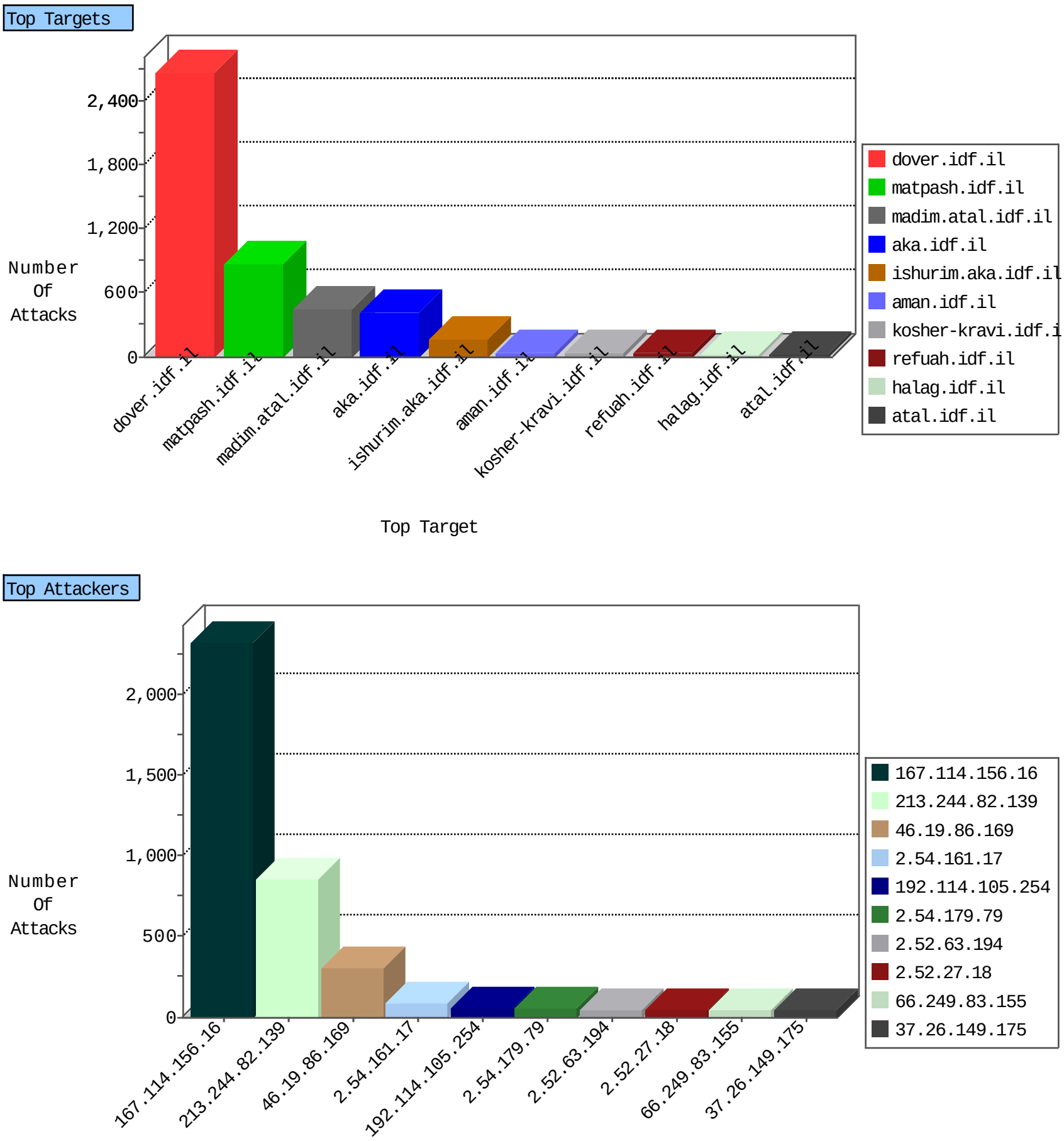
12-21-2015-09:04:09 to 12-21-2015-10:04:09

IDF Under Attack
Daily Report



12-21-2015-09:04:09 to 12-21-2015-10:04:09

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	3241
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	299
8.37.235.181	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
213.244.82.139	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
75.72.78.245	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

12-21-2015-09:04:09 to 12-21-2015-10:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.187	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-21-2015-09:04:09 to 12-21-2015-10:04:09

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	3
176.13.10.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.178.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.205.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.6.202.63	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
46.210.129.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
152.62.109.207	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
147.236.238.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.89.123	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
52.6.202.63	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.190.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.187	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1

12-21-2015-09:04:09 to 12-21-2015-10:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
213.244.82.139	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	859
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
2.54.179.79	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
79.178.15.2	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
46.19.86.121	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
8.37.235.181	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
2.52.63.194	Israel	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
2.54.161.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.54.161.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
2.54.161.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	17
2.54.161.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
84.95.215.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
37.26.149.175	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
37.26.149.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
37.26.149.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
2.54.161.17	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	13
46.19.85.120	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.83.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.182.165.60	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.80.29.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
66.249.83.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
66.249.83.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
66.249.83.155	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
66.249.83.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.161.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
212.68.153.181	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
79.178.29.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.179.79	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.226.17.54	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.131.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.15.2	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.130.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.178.61.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.149.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.145	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.179.79	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.63.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

12-21-2015-09:04:09 to 12-21-2015-10:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	200
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	111
2.52.27.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
109.253.194.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
176.13.17.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Distributed Illegal HTTP Version	Block	3
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	3
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	3
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Distributed Abnormally Long Request	Block	3
109.253.213.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 83.130.111.21	Block	2
80.246.137.203	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
89.139.149.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
180.183.2.170	Thailand	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 83.130.111.21	Block	2
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in URL from 83.130.111.21	Block	2
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method hÃ«[[#16]][[#20]]Ã¾[[#20]]Â'Ã·ÃŽÃ™!ytÂ"Ã‹Â³Â£.ÃšÃštÃµP2$Ã°?Â»Ã¤Â Ãƒ[[#25]]j5'ÂŸÃ¬[[#1]]Ã^Ã?YbÂ-sÃœÂ©(oÂ¿$Â¿2Â¹Â§O4Ã¼SÃ²/Â°Âƒ Ã®PÃ½@WÃ¨R[[#1]]F[[#4]]UGÂšÃ¥E.Ã¸ qÃ«Â°R,Â©Â• [[#11]],[WU[[#26]]xÃ?	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1387-he/refuah.aspx	Block	1
176.12.136.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.105	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	1
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	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.95	Block	1
84.108.184.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
80.246.139.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	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
2.54.162.229	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 1	Block	1
70.39.157.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23026-he/dover.aspx×"×ž×"×¨×™×š	Block	1
46.35.253.161	Russian Federation	147.237.76.42	refuah.idf.il	Parameter Type Violation &l in refua.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
82.80.17.163	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.143.85.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.250	Israel	147.237.76.42	refuah.idf.il	Malformed URL asp.net_sessionid=rgs3gt55c2zmxvby0ozyanns;	Block	1
94.230.93.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.10.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.115.83.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
37.142.132.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 83.130.111.21 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
2.52.56.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
83.130.111.21	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Name â€¹Ã™Ö¼[[#15]]Â?Â²×©â€š[[#16]]}Â?×§lAZÂ?Ã·×'â€¡ÖµÂ»×›Ë†Ë†Ö¼38×©V;[[#12]]â€ ¹wÖµ1e[[#7]]Ö²×²[[#7]]Ö¹Ã§&Â²Â¿â€?[[#12]]K ×¡_b8 in ÂŽ 4Â?iÂ?>Â´(yc[[#2]]Â¢â€"×"Â-Â¡Ö´×²Ã›b0!×›j×¨pÂ§Ö²y8fÃ¿[[#14]]^1Â§	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.12.149.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
82.81.38.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.134	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valta	Block	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

12-21-2015-09:04:09 to 12-21-2015-10:04:09