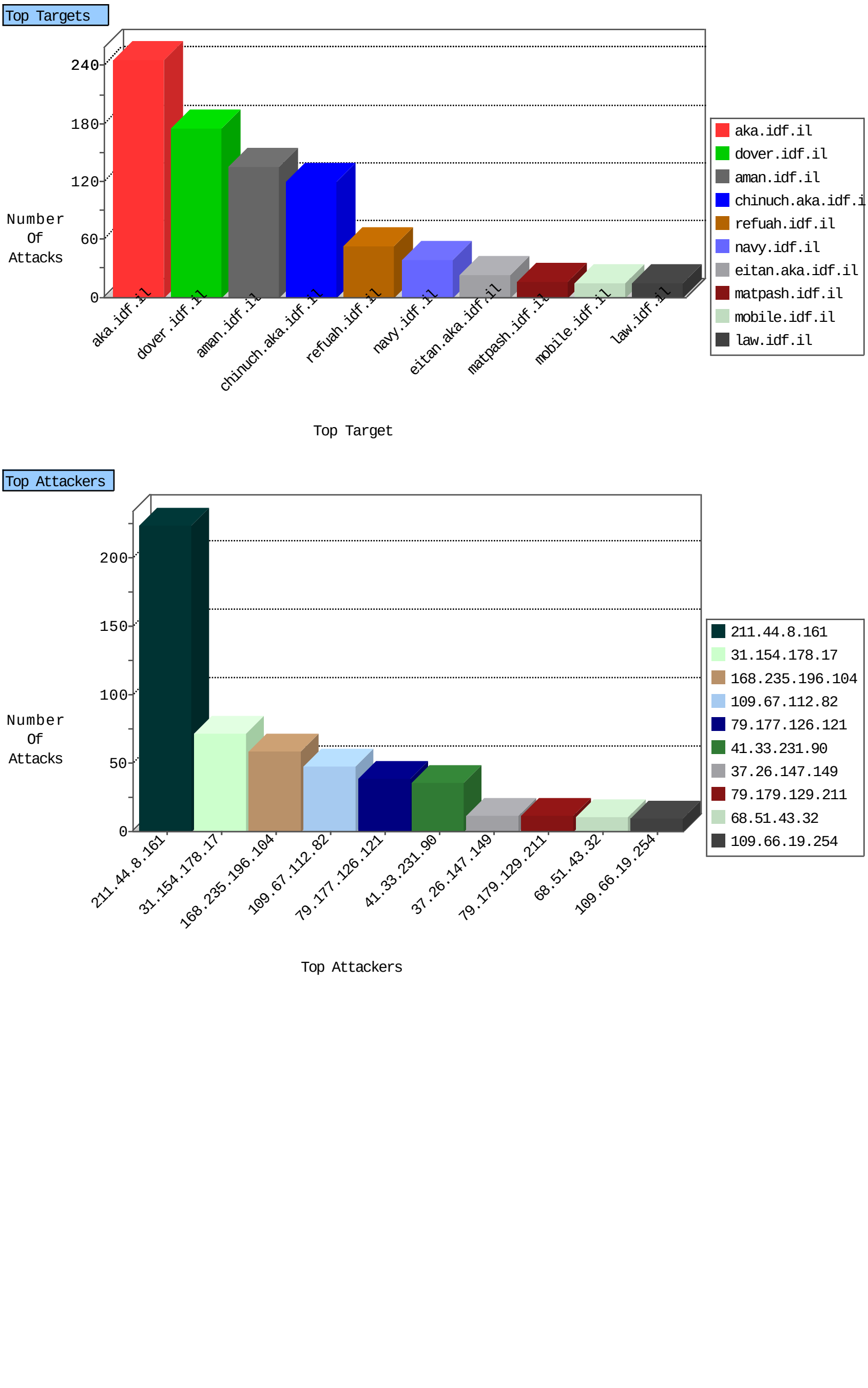
02-05-2016-17:04:03 to 02-05-2016-18:04:03

IDF Under Attack
Daily Report



02-05-2016-17:04:03 to 02-05-2016-18:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1329
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
71.83.52.230	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
168.235.196.104	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
66.249.81.212	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

02-05-2016-17:04:03 to 02-05-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
182.50.130.136	Singapore	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-05-2016-17:04:03 to 02-05-2016-18:04:03

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
66.249.78.29	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
89.248.172.173	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.226	Turkey	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
177.240.240.219	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.236.75.201	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.45.137.67	147.237.77.74	Turkey	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.236.75.201	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

02-05-2016-17:04:03 to 02-05-2016-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
211.44.8.161	Korea, Republic of	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	107
211.44.8.161	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	106
31.154.178.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
168.235.196.104	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
109.67.112.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.177.126.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
79.177.126.121	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
79.179.129.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.34.23.26	Jordan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.42.56	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.183.97.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.8.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.239.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
211.44.8.161	Korea, Republic of	147.237.72.156	aman.idf.il	SYN Attack		reject	5
93.157.84.33	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
211.44.8.161	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	5
80.246.139.116	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.121.209.177	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.120.228.39	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.198	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.145.59	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
147.236.254.11	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.54.146.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.148.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.144.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.15.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.110.108.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.177.97	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.104.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.176.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.120.228.39	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.39.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.254.75	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.34.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.181.16.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
105.200.64.238	Egypt	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.177.115.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.19.254	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	5
109.66.19.254	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	5
79.183.215.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
109.67.112.82	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.181.197.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name Ã.Âˆ Â?fÂ¬Ã°Âª[[#2]]Â?[[#4]][Â»Â€Ã¢Â½%$[[#11]]l[[#20]][[#0]]Â¢0=Ãž Â£[[#12]][[#16]][8Ã«Ã„Ã˜\Ãº	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59391&docid=65396	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in Method Â˜Â':X	Block	1
85.64.207.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/sip_storage/	Block	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
40.77.167.0	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.253.141.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Value	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in URL	Block	1
87.69.61.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	Unauthorized Method POST for 147.237.76.86/	Block	1
46.19.86.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
149.78.50.95	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$1 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.108.8.74	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Unknown HTTP Request Method Â˜Â':X	Block	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡ in URL	Block	1
65.132.59.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
84.111.136.181	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$15 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	Malformed URL	Block	1
190.171.118.222	Costa Rica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 190.171.118.222	Block	1
5.29.200.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.99.82	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58562&docid=35703	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Abnormally Long Request method	Block	1
84.228.52.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
68.51.43.32	United States	147.237.76.86	navy.idf.il	NULL Character in Header Name at Ã…Â^Â?fÂ¬Ã°Âª[[#2]]Â?[[#4]][Â»Â€ Ã¢Â½%$[[#11]]l[[#20]][[#0]]Â¢0=ÃžÂ£[[#12]][[#16]][8Ã«Ã„Ã˜\Ãº	Block	1
190.171.118.222	Costa Rica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish/	Block	1
37.142.142.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-05-2016-17:04:03 to 02-05-2016-18:04:03