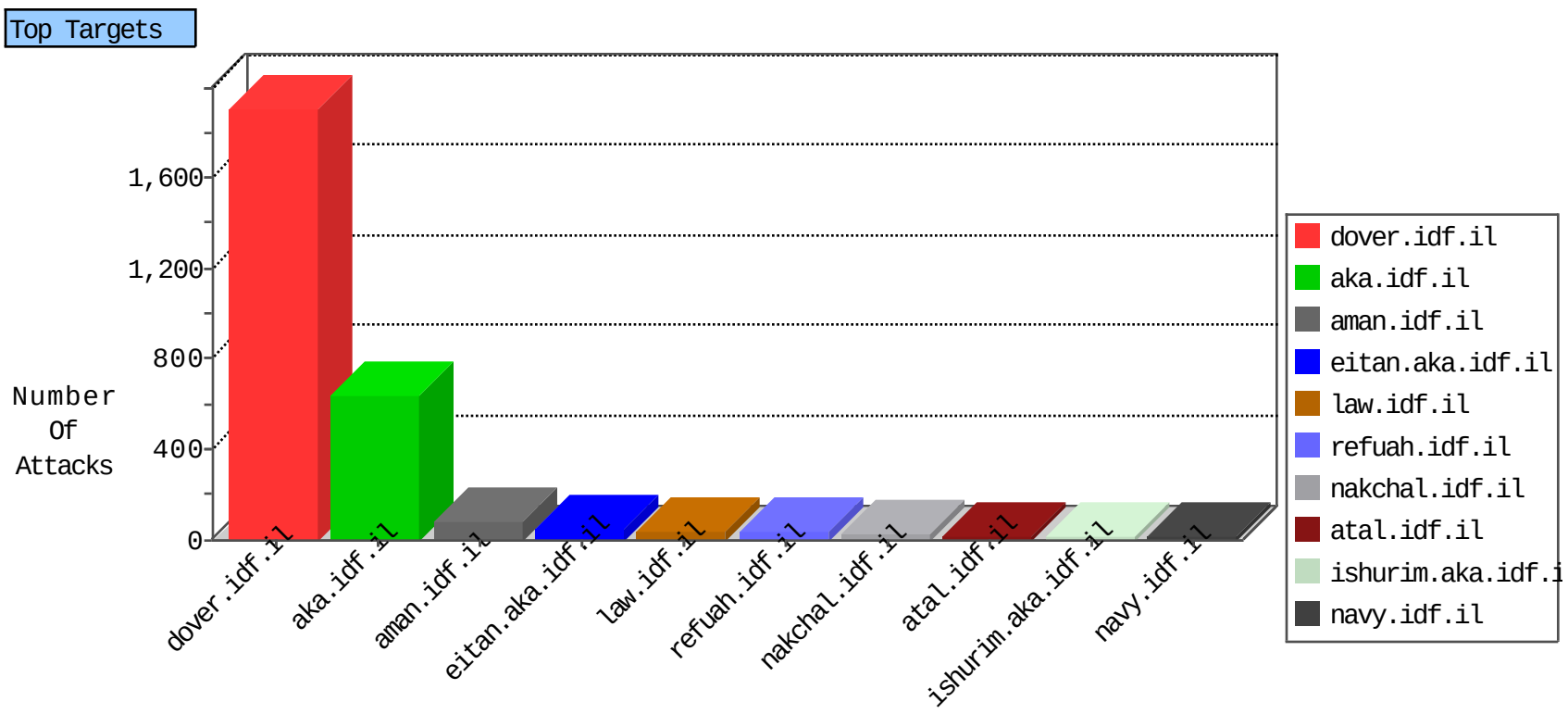
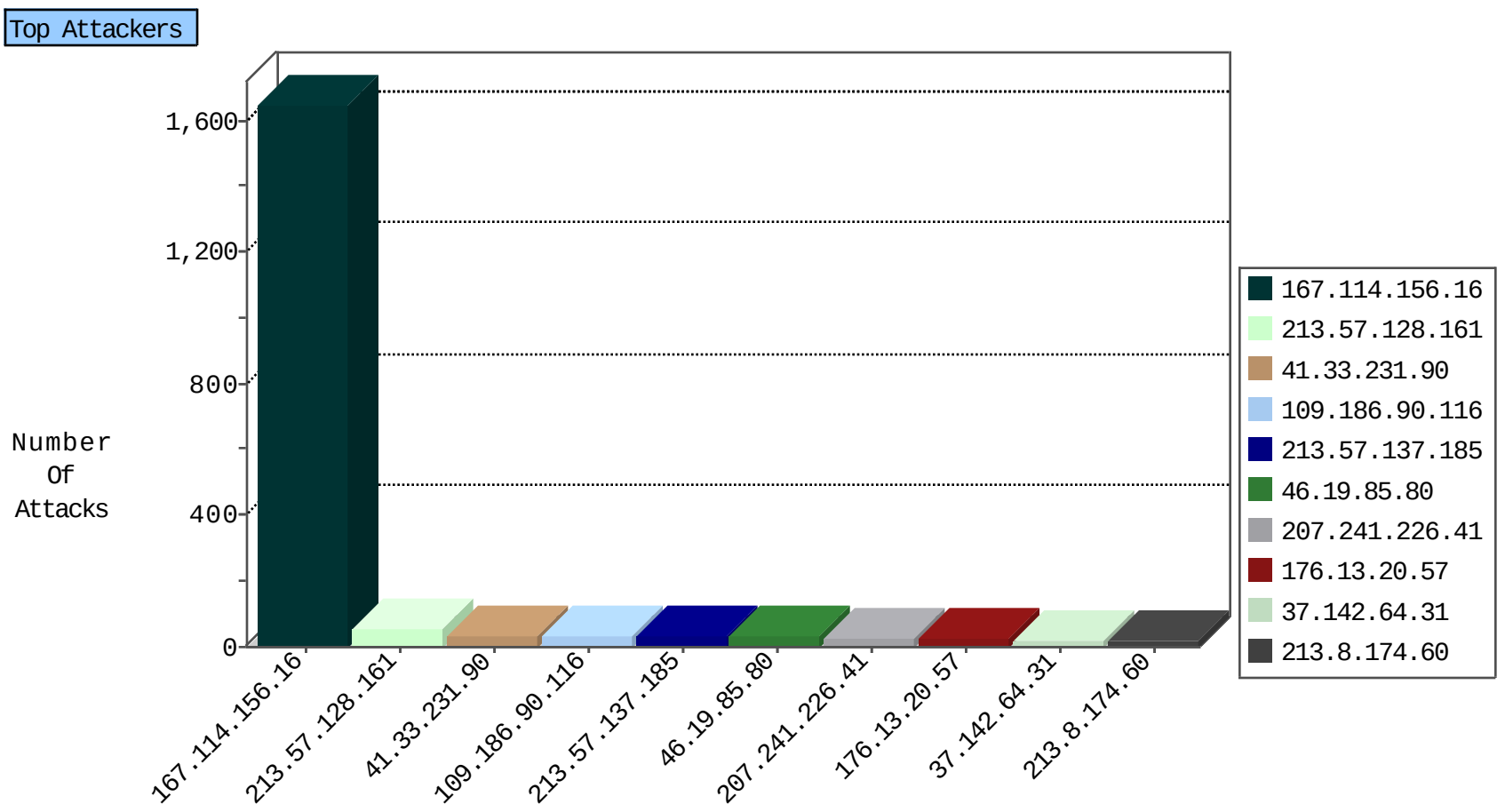
12-05-2015-14:04:06 to 12-05-2015-15:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-05-2015-14:04:06 to 12-05-2015-15:04:06

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	3213
95.35.194.137	Israel	147.237.72.166	aka.idf.il	block-sp-traf1	drop	3
146.185.239.100	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1

12-05-2015-14:04:06 to 12-05-2015-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-05-2015-14:04:06 to 12-05-2015-15:04:06

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
66.249.66.75	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.120.82	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
95.211.120.82	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
85.93.88.114	147.237.77.121	Germany	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.108.132.58	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.120.82	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1

12-05-2015-14:04:06 to 12-05-2015-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.128.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.8.204.47	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
80.246.130.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
176.13.20.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
37.142.64.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
185.120.125.6		147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
207.241.226.41	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
207.241.226.41	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
213.8.174.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
213.8.174.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.108.116.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
217.132.3.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.235.31.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.38.184	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.137.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
5.102.254.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.13.113.92	Ireland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
173.252.74.115	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.12.143.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.20.70	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.120.131.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.24.181.135	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
65.255.52.229	Turks and Caicos Islands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
40.77.167.73	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.142.64.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.208.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.170.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
40.77.167.73	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.185.151.123	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
79.176.131.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.116.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.137.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.24.181.134	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.182	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.115	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.137.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.93.234	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.196	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.154.170.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.13.113.66	Ireland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.157.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.13.113.87	Ireland	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

12-05-2015-14:04:06 to 12-05-2015-15:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.186.90.116	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.90.116	Block	28
162.203.2.233	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 162.203.2.233	Block	9
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	3
37.26.148.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.148.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
162.203.2.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
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
2.54.11.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.67.168	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	2
31.154.170.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.98	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
77.125.130.58	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/61246.gif	Block	1
207.46.13.143	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.130.233	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.125.130.58	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Â¢=R,Â¥Ã«Ã§0Ã–[[#6]]7Ã¬cÃ…ÂœÂ’ Â°g[[#15]]Â?!Â¦Ã£%ÃŠ[[#22]]^[[#31]] Â¸ ÂŒÂ¥[[#14]]3Ã¥[[#30]]G[[#28]]]Â•Ã©Ã•[xÂ”Ã‰Ã´Ã… Â¦z[[#19]][[#16]]Â”Ã«;O[[#5]])>Â”PZ[[#12]]<hr%Ã‘Ã‘,=Â»Â«F;`Â?Ã– >[[#28]][[#24]]RÃ˜ÃšÂ§Ã½>RÂ°Ã·4Âš[[#16]]Ã·ÂŽYÂ‡ Ã¹VÃ¯e[[#19]]Ã¬w[[#6]](Â¬[[#8]]sBr!rÂ½r[[#16]]Â-ÃšÂ•v?Ã’ÂŽaÂ‡Ã‰Ã, Ã–Ã°37[[#6]]ÃŒ=Ã¨0Ã²Ã’ÃžÂ›] in URL tâ€°ÃŸÂ®[[#6]][[#29]]	Block	1
37.26.149.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
162.243.188.75	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /	Block	1
77.125.130.58	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
109.201.152.22	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.65.84.183	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.67.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8762-he/refuah.aspx	Block	1
213.57.204.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.0.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.26.147.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.115	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
77.125.130.58	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 7	Block	1
77.125.98.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17802-he/dover.aspx	Block	1
207.241.226.41	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
84.94.15.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.157.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.246.96.76	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
77.125.130.58	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â¢=R,Â¥Ã«Ã§0Ã–[[#6]]7Ã¬cÃ…ÂœÂ’Â°g[[#15]]Â?!Â¦Ã£%ÃŠ[[#22]]^[[#31]] Â¸ ÂŒÂ¥[[#14]]3Ã¥[[#30]]G[[#28]]]Â•Ã©Ã•[xÂ”Ã‰Ã´Ã… Â¦z[[#19]][[#16]]Â”Ã«;O[[#5]])>Â”PZ[[#12]]<hr%Ã‘Ã‘,=Â»Â«F;`Â?Ã– >[[#28]][[#24]]RÃ˜ÃšÂ§Ã½>RÂ°Ã·4Âš[[#16]]Ã·ÂŽYÂ‡ Ã¹VÃ¯e[[#19]]Ã¬w[[#6]](Â¬[[#8]]sBr!rÂ½r[[#16]]Â-ÃšÂ•v?Ã’ÂŽaÂ‡Ã‰Ã, Ã–Ã°37[[#6]]ÃŒ=Ã¨0Ã²Ã’ÃžÂ›]	Block	1
2.54.47.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.43.215	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
87.68.70.179	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8911-he/refuah.aspx	Block	1
213.151.37.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.166.190.145	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
185.120.125.25		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.129.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.163	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	1

12-05-2015-14:04:06 to 12-05-2015-15:04:06

12-05-2015-14:04:06 to 12-05-2015-15:04:06