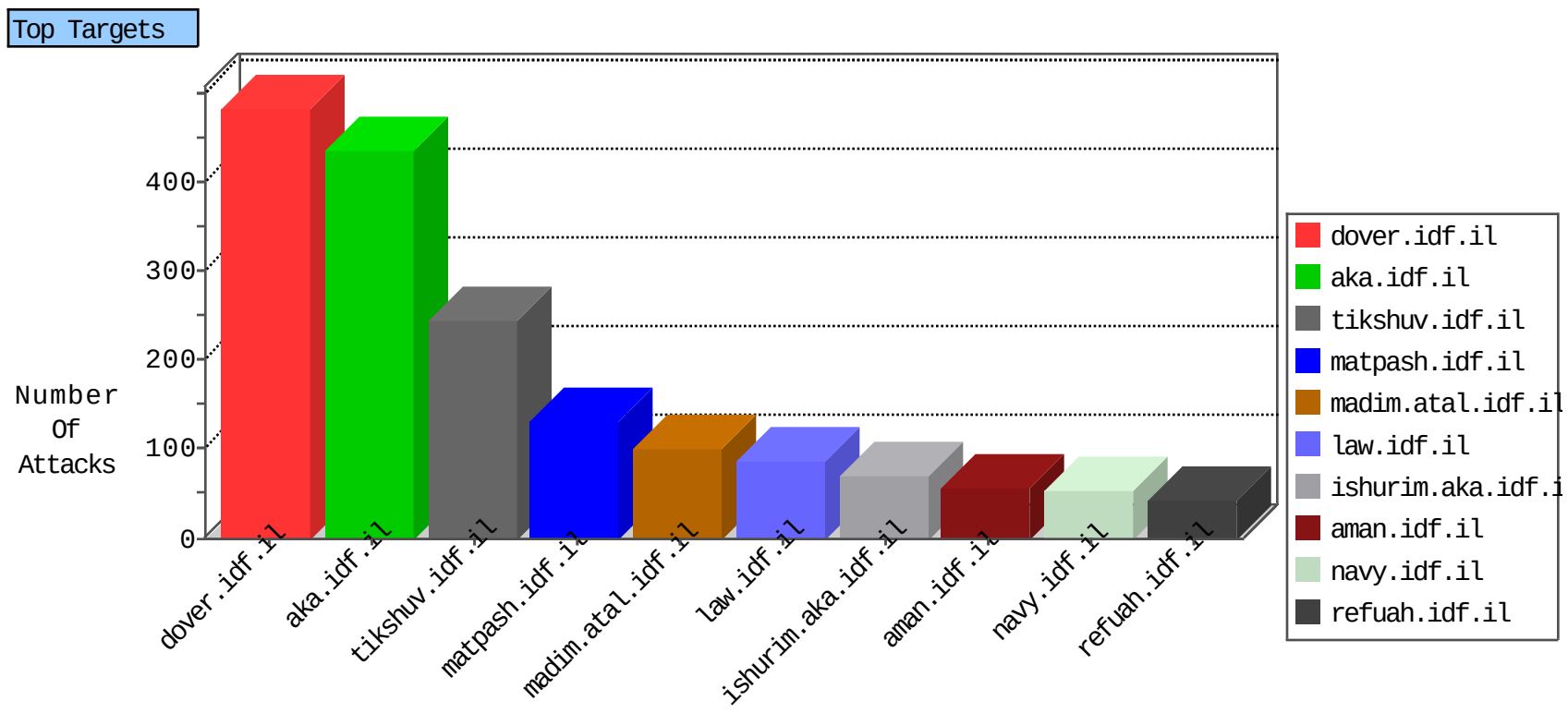
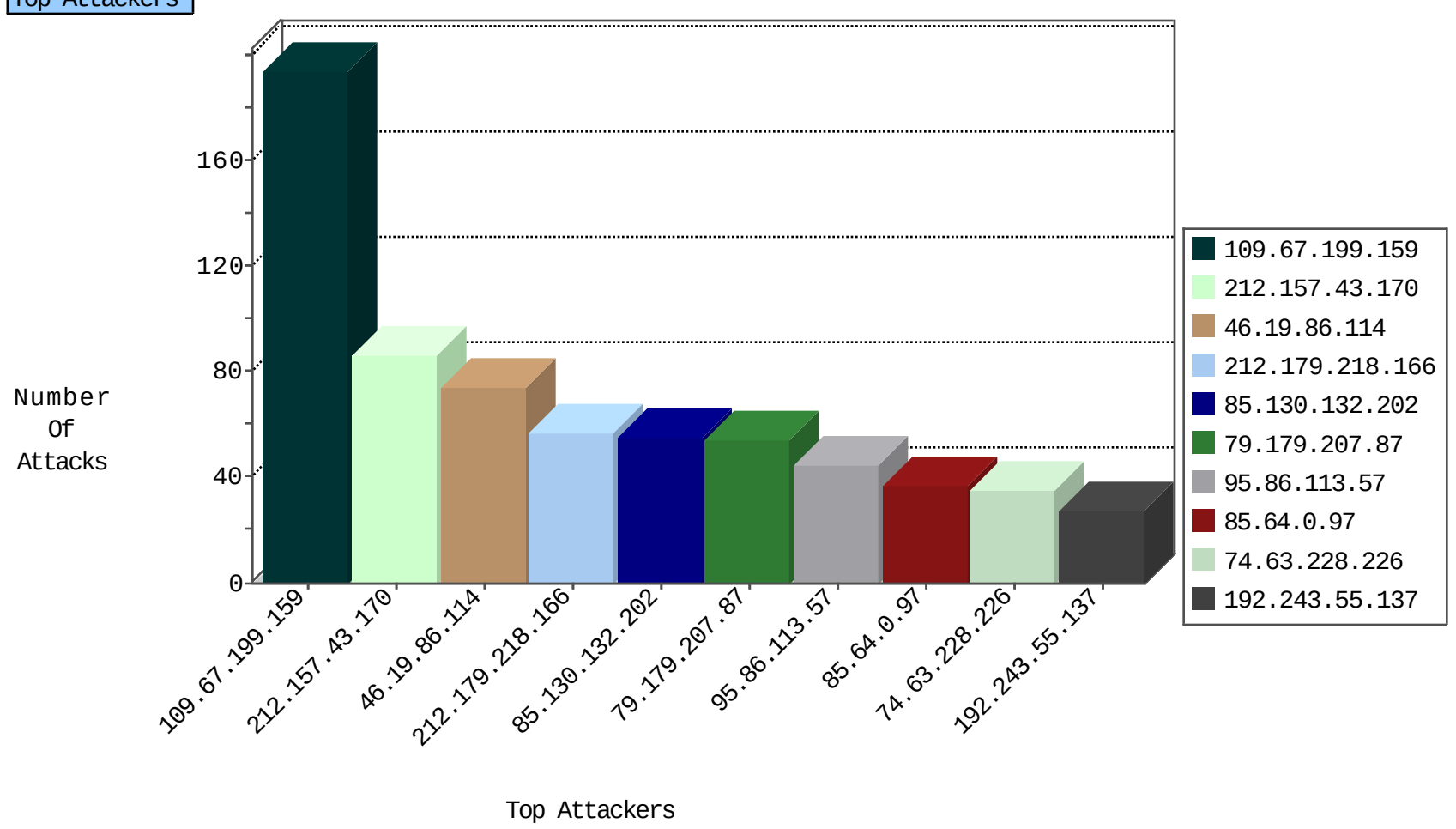
02-18-2016-14:04:06 to 02-18-2016-15:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-18-2016-14:04:06 to 02-18-2016-15:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
79.179.207.87	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	36
79.179.207.87	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	18
79.177.236.233	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
185.130.5.179		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
45.32.161.174		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
45.32.161.174		147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
45.32.161.174		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
37.59.28.127	France	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

02-18-2016-14:04:06 to 02-18-2016-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.79.150	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	11
74.63.228.226	United States	147.237.77.226	www.chamatz.aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	9
74.63.228.226	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
149.88.146.149	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
138.134.102.16	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	5
177.185.194.45	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
85.65.38.41	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
46.137.81.122	Ireland	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
195.140.210.83	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.76.174.2	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
109.67.165.182	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	4
74.63.228.226	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.137.81.122	Ireland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.145.99	Israel	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
74.63.228.226	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.204.76	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
70.89.127.77	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
216.10.220.154	Jamaica	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.67.53.172	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
109.67.165.182	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
70.89.127.78	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
74.63.228.226	United States	147.237.77.226	www.chamatz.aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

02-18-2016-14:04:06 to 02-18-2016-15:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.137.81.122	147.237.77.74	Ireland	law.idf.il	SQL Injection - Select From	17
66.76.174.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
195.140.210.83	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	7
203.171.41.47	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	5
70.89.127.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
70.89.127.78	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	2
93.174.95.119	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.81.250.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.76.196.138	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.150.143.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.95.119	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.133.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-18-2016-14:04:06 to 02-18-2016-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.157.43.170	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	84
109.67.199.159	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
85.64.0.97	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.246.130.36	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
2.54.17.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
217.194.207.140	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
85.130.132.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
5.29.123.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.130.132.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
87.68.248.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
74.63.228.226	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
132.73.204.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.130.132.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.29.123.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
195.160.242.40	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.49.45	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
41.217.160.169	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.64.0.97	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
177.63.5.166	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.130.132.202	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.133.127	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.226	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.138.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.73.204.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.79.150	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.201.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.226	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.1.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.17.42.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.143.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.148.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.223.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.134.197	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
109.253.138.160	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.155	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

02-18-2016-14:04:06 to 02-18-2016-15:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.199.159	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	135
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
194.54.168.65	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 194.54.168.65	Block	7
176.13.13.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.100	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	4
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 95.86.113.57	Block	3
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 95.86.113.57	Block	3
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
176.13.15.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 95.86.113.57	Block	3
176.13.18.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 95.86.113.57	Block	3
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 95.86.113.57	Block	3
46.19.85.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 95.86.113.57	Block	2
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
131.253.25.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 95.86.113.57	Block	2
149.88.124.126	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
2.54.190.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 95.86.113.57	Block	2
87.69.166.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.114.3	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 80.179.114.3	Block	2
37.26.146.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
74.84.136.105	United States	147.237.72.166	aka.idf.il	Multiple signatures from 74.84.136.105	Block	1
66.249.64.175	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request request version	Block	1
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version [[#25]]txB>Â•.][[#24]]Ã£Â•ÃŠÃ‡Ã¥S/[[#30]]Â²Âœ Ã?0Â®Ã–RÃ°o[[#15]]Ã²S=Â-3[[#16]][[#3]][[#15]]Â€Â¨Ã¦Â«`ÂŠÂ… [[#30]]?ÂŽv7Ã¹[[#28]]Ã–Ã¬CÃ„Â›Â±[[#25]]eÂ»Â›:uÃ‹[[#15]]Ã³/Ã^ [[#17]]eÂ¶Ã?Â°Â?Â‰PÃ‰Ã¢Ã§Ã?Ã·=ZÃšÂ¿Ã€Â°Â¼Ã,	Block	1
93.182.192.2	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin2.wmv http:/opensky-media.com/de/arunachalashiva/excerpts.php	Block	1
98.19.222.133	United States	147.237.72.156	aman.idf.il	Multiple signatures from 98.19.222.133	Block	1
80.179.114.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1640.jpg	Block	1
178.63.18.196	Germany	147.237.72.166	aka.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
197.48.238.133	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.142.220.18	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Âª Â“*8bÂ§u%Â¹Â-Ã‹)Â•[SÃœ[[#4]]Â‹ [[#6]]Ã»[[#2]]Ã½f[[#2]]@Â?[[#17]]Âµ;[[#6]]ÃµÃˆÃ?[[#27]]%ÃŒ in URL Âœ Â¿eb×°[[#1]][[#0]]r\[[#0]]h×ƒ× d>â€Ž[[#23]]kÃ·iÃ»â€œ×€[[#23]]Ã·câ€ ?Ö°×œf â„¢×¨	Block	1
85.130.132.202	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
192.114.175.66	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
79.180.38.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ain/home/default.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method Â¶bL	Block	1
95.86.113.57	Israel	147.237.72.166	aka.idf.il	Illegal Parameter Encoding â,¬[[#28]]zP;W!W×˜}×?r1[[#17]]'Â»/Ãœ[[#17]]×’ Â¨!Â§×¤Â©qN^Ö±Ö±SÂ¬[[#23]]Ö³.ÂŠÂŒ×š×ª2w[[#23]]×ƒ×– [[#7]]Ã·*[[#25]][K[[#7]]×€[[#6]]CÂžE} Â´Öµâ€?â€”â€?×¨×´Ö¸YÂµlÃœ "Ö±e3ÃŠHm[[#30]]ÂŽÖ¶Â£?ÂŒ×±[[#29]]QÂ?â€šU;Ö´J×¨,2[[#6]]SÖ°Â?RË† Â±qX%â€¹.5[[#30]]NÂ¨mâ€œsâ€”Ãš×,8[[#4]]Â³Â®[[#14]]×œ Ã·[[#31]]Â°#ZÂ?×ªdâ€¢â€šÂ¥[[#21]]`8[[#15]]Ãž#Ãœ[[#18]]c[[#2]]×¦Ã–gÃš	None	1
93.182.192.44	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/16.stmus005/pages/default.aspxttywotion	Block	1

02-18-2016-14:04:06 to 02-18-2016-15:04:06