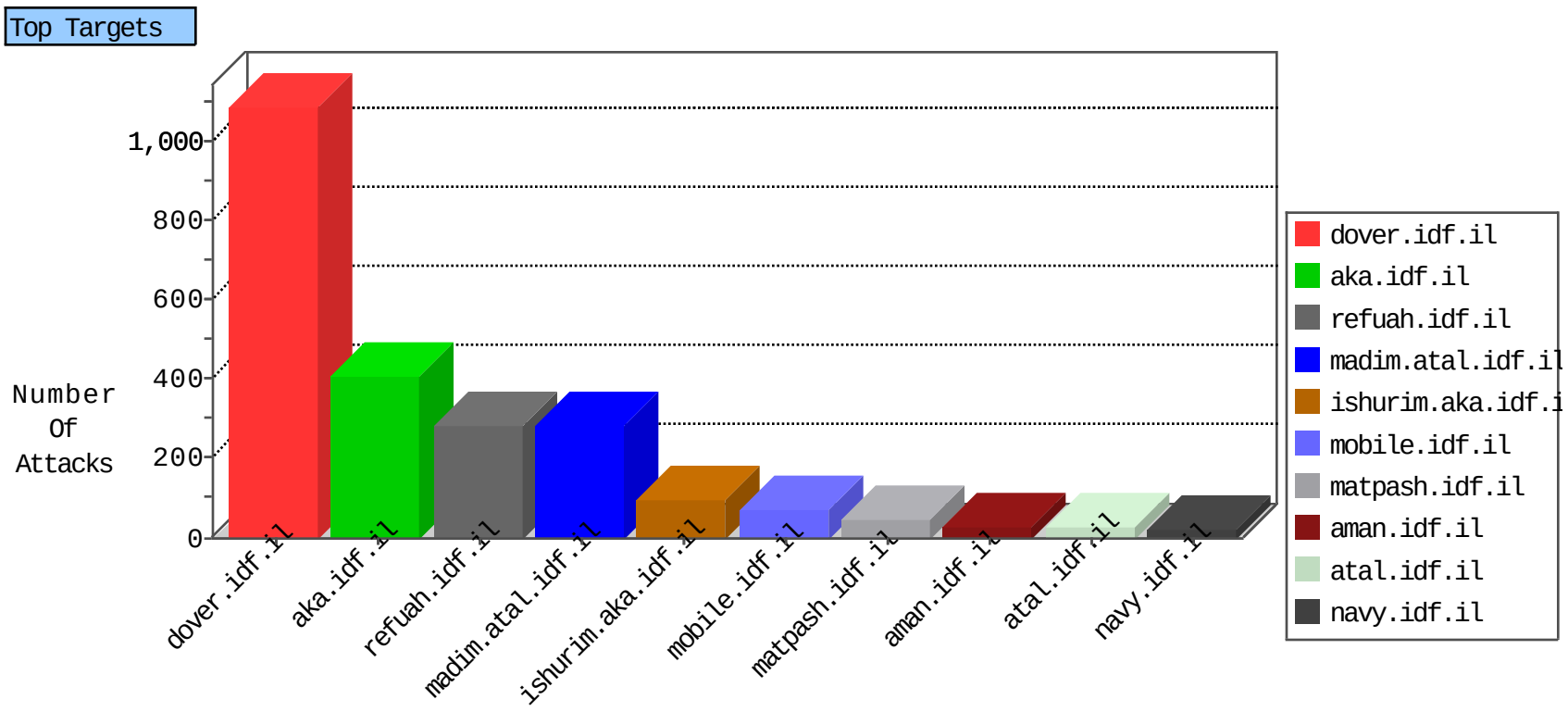
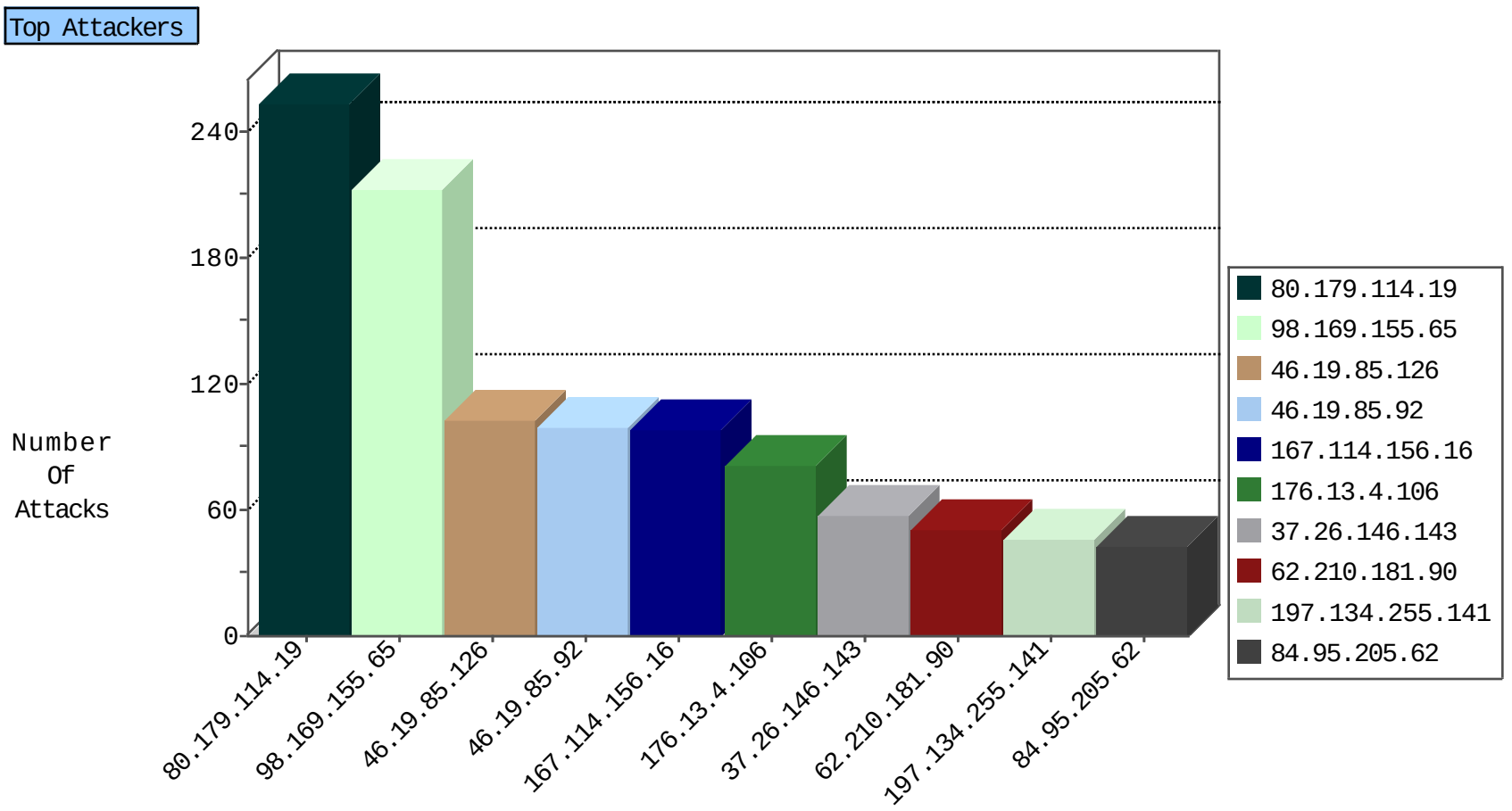
05-03-2016-15:04:08 to 05-03-2016-16:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-15:04:08 to 05-03-2016-16:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	2984
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2640
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	41
79.183.129.25	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
71.6.216.54	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.48	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-15:04:08 to 05-03-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-15:04:08 to 05-03-2016-16:04:08

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	2

05-03-2016-15:04:08 to 05-03-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.179.114.19	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	249
98.169.155.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	196
176.13.4.106	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
37.26.146.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
62.210.181.90	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
197.134.255.141	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.78.223	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
84.95.205.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
47.23.170.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.183.11.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
95.130.89.4	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
66.249.78.90	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
88.150.202.85	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
188.32.69.66	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.26.149.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
98.169.155.65	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	17
85.65.10.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
107.170.68.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.179.140.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.235.98.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
176.13.6.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.156.234	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.154.17.194	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	11
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.254.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.78.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.149.193.5	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
66.249.78.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.76.127.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.219.137.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.226.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.158.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.8.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.210.148.246	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
176.13.15.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
109.65.147.34	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	11
2.53.158.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
80.246.139.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.128.84	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	8
80.246.136.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
2.55.152.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	4
109.65.147.34	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/7/	Block	3
88.150.202.85	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
82.81.109.130	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.108.68.81	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	3
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.23.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.146.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/schar	Block	2
65.55.213.28	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.93.113	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/contactus/mobile	Block	2
31.154.33.190	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized HTTP Method	Block	2
94.188.164.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Illegal HTTP Version +iw test :Test Wuz Here	Block	1
66.249.78.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-23050-he/dover.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-23150-he/dover.aspx	Block	1
212.179.21.194	Israel	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method dHlsZQUOY3Vyc29yOmRlZmF1bHQfCQUSamF2YXNjcmlwdDp2b2lkKDApHwoFygFzZXRDbGFzc0ZvckZvdXJ0aExldmVsKCdjdGwwMF91Y011bHRpU2lkZUJhcl9nZW5lcmFsU2lkZUJhcl9zcGNEZXRhaWxzX3JwdFN1YkNhdGVnb3JpZXNfY3RsMDBfc3BjRGV0YWlsczJfcnB0U3ViQ2F0ZWdvcmllc19jdGwwMV9zcGNEZXRhaWxzM19ycHRTdWJDYXRlZ29yaWVzX2N0bDAwX2xpTWVudUl0ZW1XcmFwcGVyJywnc19tX2xldl8zX2xpX29uJyk7HwsFxwFzZXRDbGFzc0ZvckZvdXJ0aExldmVsKCdjdGwwMF91Y011bHRpU2lkZUJhcl9nZW5lcmFsU2lkZUJhcl9zcGNEZXRhaWxzX3JwdFN1YkNhdGVnb3JpZXNfY3RsMDBfc3BjRGV0YWlsczJfcnB0	Block	1
85.64.6.11	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.75.78.171	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
31.154.33.190	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/0/	Block	1
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Multiple Malformed HTTP Header Line from 118.193.27.6	Block	1
66.249.78.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-23122-he/dover.aspx	Block	1
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Abnormally Long Header Line request header name	Block	1
95.86.125.75	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
62.219.99.154	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.99.154	Block	1
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Malformed HTTP Header Line 2	Block	1
66.249.93.109	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10653-he/dover.aspx	Block	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	1
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
85.65.10.20	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.179.114.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Multiple Malformed URL from 118.193.27.6	Block	1
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Abnormally Long Request method	Block	1
66.249.78.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10655-he/dover.aspx	Block	1
95.170.149.44	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/66846.ppt'a=0	Block	1
192.115.200.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl95 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
118.193.27.6	Hong Kong	147.237.77.19	law-forum.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#1]]"[[#1]][[#0]][[#1]][[#30]][[#3]][[#3]]:ô[[#2]]¿½M.ùü[[#29]]U51>^©8Ù[[#30]][[#27]]‘¡ë[[#6]]‡bãÇ¶Û“[[#6]][[#0]][[#0]]^À0À,À($ À[[#20]]À in URL	Block	1