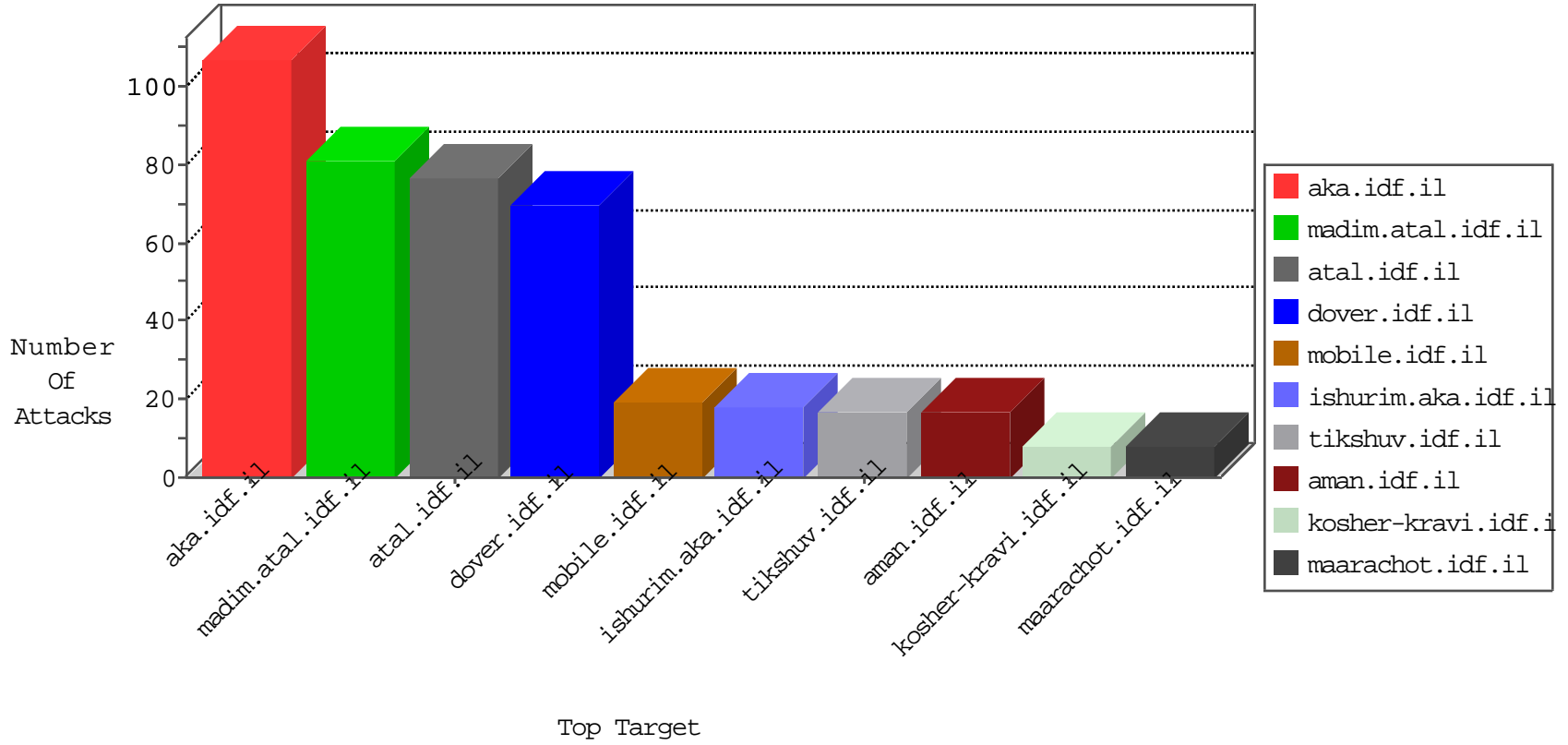


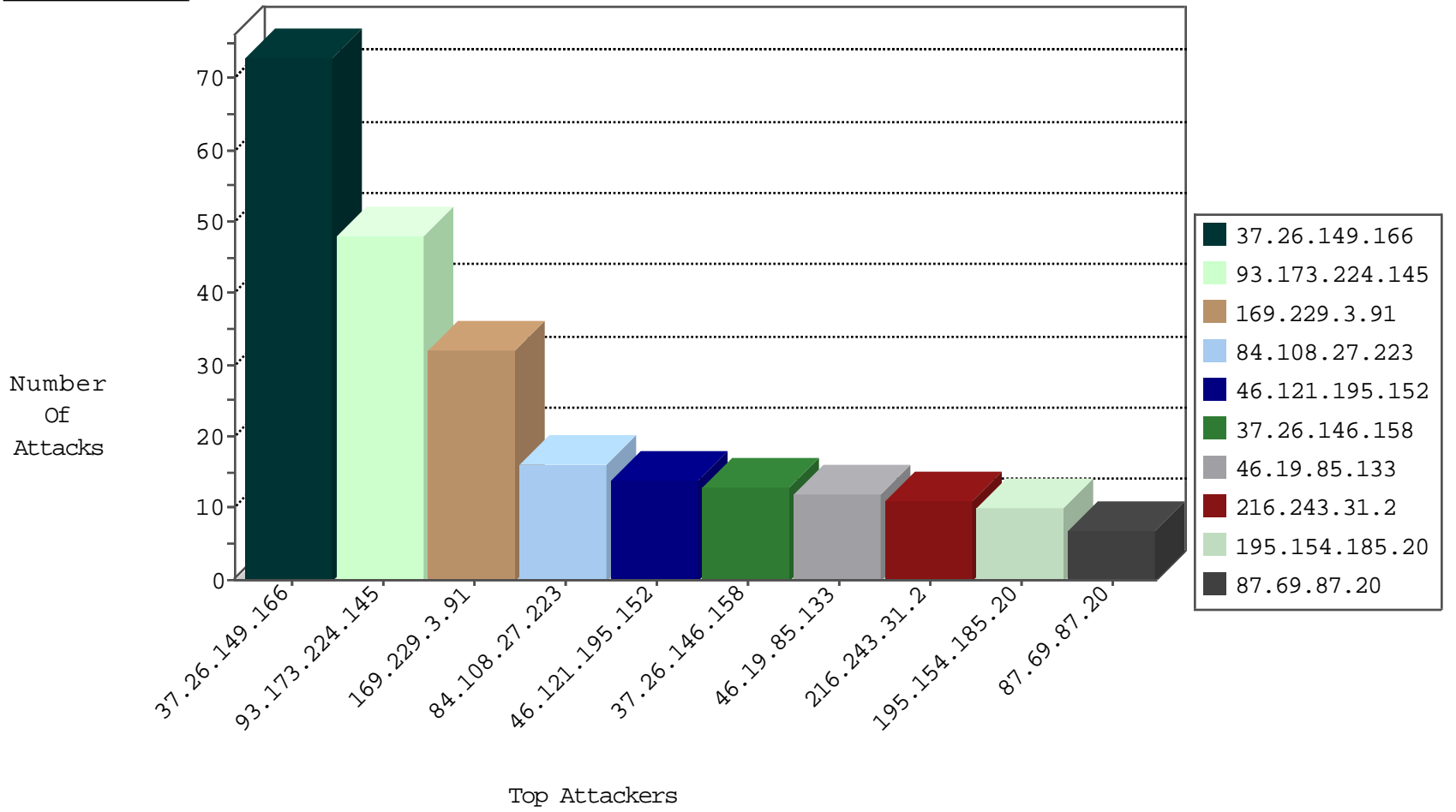
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
134.147.203.115	Germany	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	2
74.82.47.9	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.53	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
67.249.19.253	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.41.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
46.121.214.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
195.154.185.20	France	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Block	4
195.154.185.20	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
195.154.185.20	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.88.84.77	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
195.154.185.20	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.86.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
69.30.215.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1

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
37.26.149.166	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
159.122.220.108	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
186.226.85.69	147.237.77.233	Brazil	atal.idf.il	ET SCAN NMAP -sS window 1024	1
177.43.249.41	147.237.8.24	Brazil	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
177.43.249.41	147.237.8.24	Brazil	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
159.122.220.108	147.237.76.198	Netherlands	e.yohanan.idf.il	ET SCAN Potential SSH Scan	1
159.122.220.108	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
194.187.249.70	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
186.226.85.69	147.237.77.176	Brazil	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
177.43.249.41	147.237.8.24	Brazil	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
159.122.220.108	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.173.224.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
46.121.195.152	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
37.26.146.158	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.27.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.154.107	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.179.34.153	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.108.27.223	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
84.108.177.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.80.177.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.22.134.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.94.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.1.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
14.97.254.163	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.165.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.6.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.189	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.142.68.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.213	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.85.134	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.179.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.27.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
176.13.0.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.20.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.224	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
149.88.247.157	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.116.18.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
93.172.22.40	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
31.210.188.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.121.60.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.27.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.166	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	2
5.102.195.96	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.237.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.27.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.11	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.142.247.26	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.46.39.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.86.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
74.82.47.18	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.135.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
87.70.82.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.147.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
87.69.87.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.87.20	Block	6
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	3
207.241.229.49	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan/pratim/pirteyerua	Block	2
84.108.27.223	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
65.55.210.164	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Unknown HTTP Request Method	Block	1
14.97.254.163	India	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.97.254.163	Block	1
212.34.23.48	Jordan	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
157.55.39.47	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/2/112922.pdfxžx x"x™x'x•xª	Block	1
87.69.87.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/mailbox.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.66.67	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/107537.pdf	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Malformed URL '[[#6]]§ r[[#18]]i•Û[[#7]]b'fÛ	Block	1
37.142.243.213	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.88.71.234 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Abnormally Long Request method	Block	1
14.97.254.163	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/perty=	Block	1
212.34.23.48	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
93.173.224.145	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Malformed URL	Block	1
66.249.66.126	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Unknown HTTP Request Method I[[#4]]°ÁŽV0_iİ6[[#14]]¶ŪE:¶-ÁŸ¶Ōjª"vcsTñkf[[#8]]t<"! in URL ' [[#6]]§ r[[#18]]i•Û[[#7]]b'fÛ	Block	1
40.77.167.74	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
207.241.229.215	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/kadatzhelp	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
84.108.81.16	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$17 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method I[[#4]]°ÁŽV0_iİ6[[#14]]¶ŪE:¶-ÁŸ¶Ōjª"vcsTñkf[[#8]]t<"!	Block	1
37.26.146.158	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.34.23.48	Jordan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
93.173.224.145	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	NULL Character in Method [[#3]]: [[#12]]µ= [[#0]]aİ•™[[#1]]:üÁŌjª"¶ŪIq= [[#0]] [[#8]]•Ã [[#26]]- Xt [[#24]]j [[#7]]ĚñÁŌjª<!Ž? [[#15]]üŌ<†	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
46.121.195.152	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Abnormally Long Request	Block	1
207.241.229.215	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/rabanut/general.aspx	None	1
150.70.173.41	Japan	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
84.108.177.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/kapatz/default.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Method •-ē[[#2]]±@« Ōã#Ō[[#22]]ŸÃ»- [[#0]]n¶ŪE	Block	1

03-05-2016-14:04:03 to 03-05-2016-15:04:03

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Query String on '[[#6]]\$ r[[#18]]i•Û[[#7]]b'fÛ	Block	1

03-05-2016-14:04:03 to 03-05-2016-15:04:03