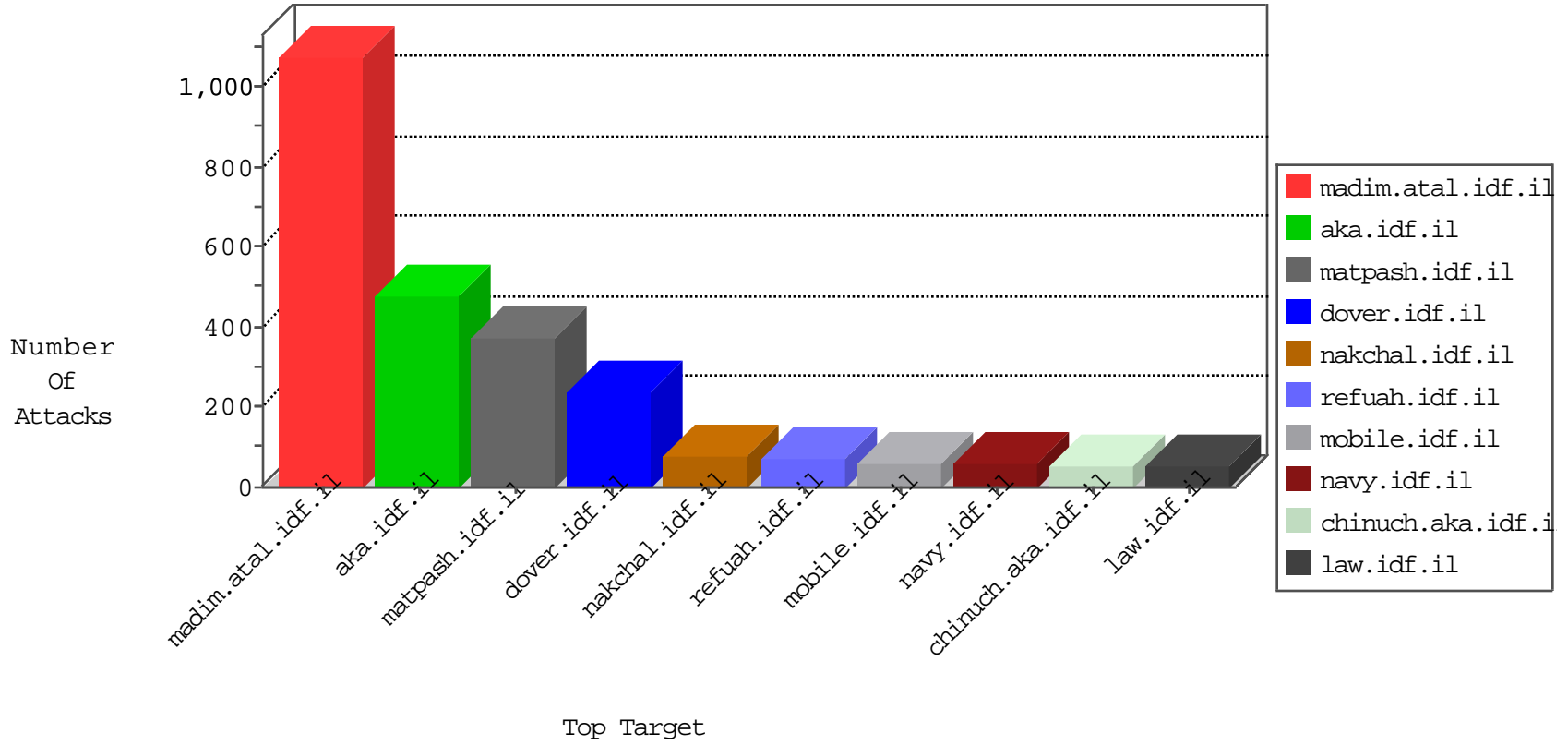


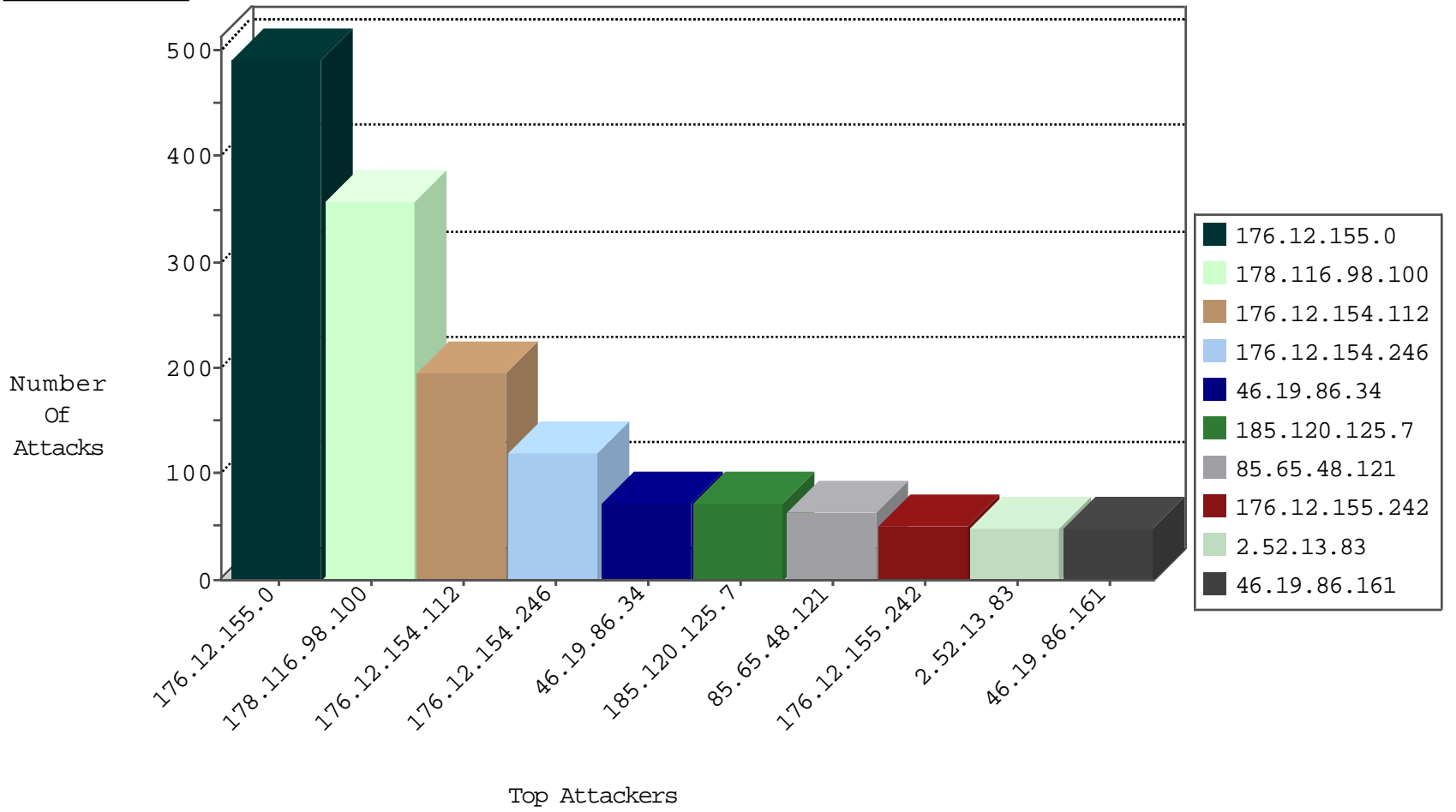
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	9
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
142.54.160.210	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	drop	1
142.54.169.166	United States	147.237.77.205	prisha.idf.il	block-sp-trafl	drop	1
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.240.235.225	Israel	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.225.121	France	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.190.233	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
109.64.163.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.172.140	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.215.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.4.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.72.14	Sweden	dover.idf.il(ol	ET SCAN NMAP -sS window 1024	1
31.168.78.253	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
185.32.179.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.216.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.0.75.114	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
95.35.4.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.172.140	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.120.120.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.178	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.97.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.116.98.100	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	357
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
2.52.13.83	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
80.246.130.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
85.65.48.121	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
85.65.48.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
46.19.86.75	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.86.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.65.164.30	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.86.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
85.130.219.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.155.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.177.9	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.130.177.9	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
85.130.177.9	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
2.54.190.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
213.55.104.210	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.151.59.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.221.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.60.96	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.7.26	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.175.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.97.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
217.132.139.249	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
176.12.154.30	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.9	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
217.132.139.249	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.12.154.30	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.9	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.186.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.198.164	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.24	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.141	Israel	147.237.77.216	dover.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
66.249.78.154	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.178.161.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
157.55.39.93	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.155.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	243
176.12.154.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	187
176.12.155.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
176.12.154.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
176.12.155.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	76
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
176.12.155.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.12.155.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
212.235.103.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	21
176.12.155.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
79.179.63.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authentication-service.asmx/getauthuser	Block	10
188.143.232.16	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.16	Block	8
192.118.64.29	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.118.64.29	Block	6
176.12.154.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
212.235.103.211	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 212.235.103.211	Block	5
176.12.154.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
176.12.154.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
76.115.96.90	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	3
176.12.155.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
79.183.0.245	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.94.181.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	2
176.12.155.147	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
194.90.151.18	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.19.85.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
176.12.154.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.40.57	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
73.172.157.202	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.65.164.30	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
46.121.158.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
182.178.76.166	Pakistan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
85.65.197.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cblQuest ion\$1 in www.aka.idf.il/main/gyus/questionnaire.aspx	None	1
5.29.194.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method Ã~ [[#4]]Ã~x[[#8]]Ã~e1Ã~tZDÃ~tgÃ~WÃ~tYyoZ[[#12]]Ã~BÃ~Ã~ rp[[#4]]D[[#17]]fÃ~Z	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
185.60.144.32	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in URL	Block	1
91.240.235.225	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/login.aspx	Block	1
217.194.203.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
41.189.33.157	Cote D'Ivoire	147.237.77.233	atal.idf.il	E-mail collector robots 14	Block	1
2.52.138.65	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1