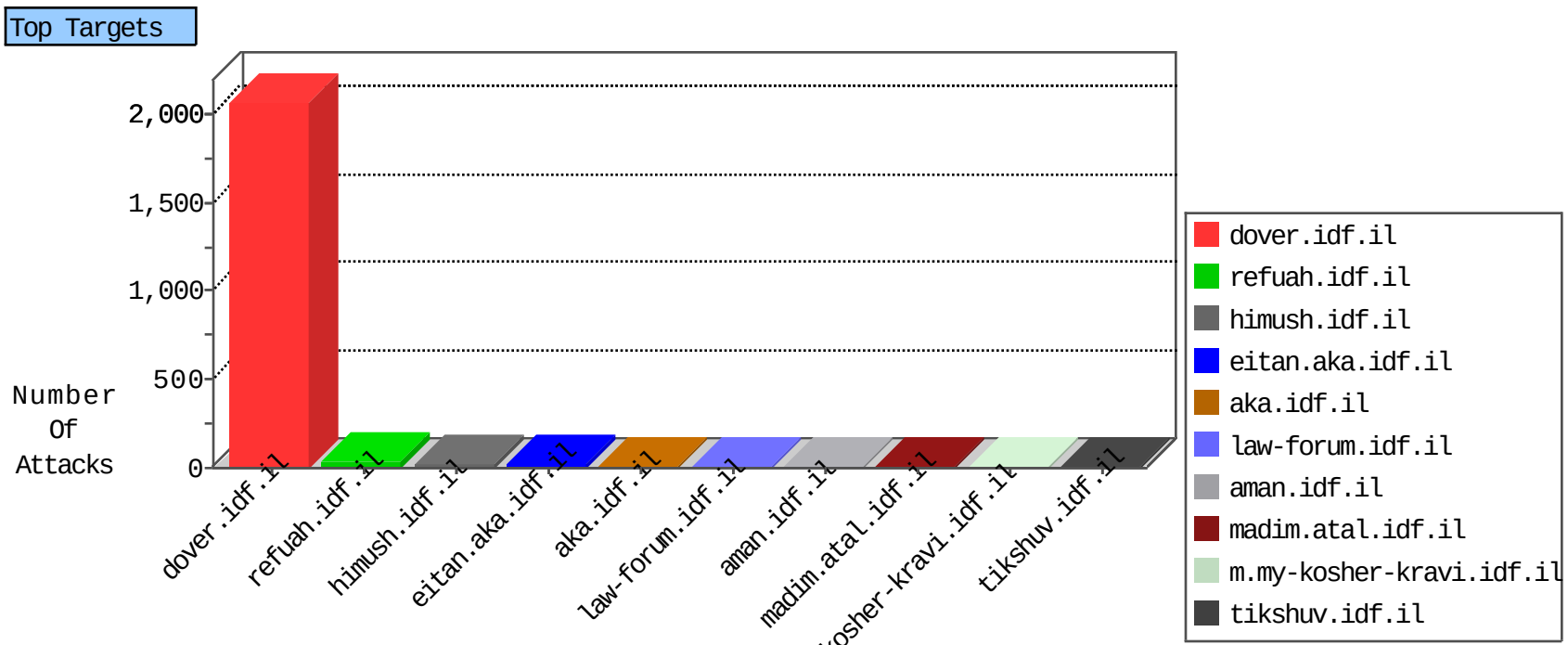
01-18-2016-03:04:00 to 01-18-2016-04:04:00

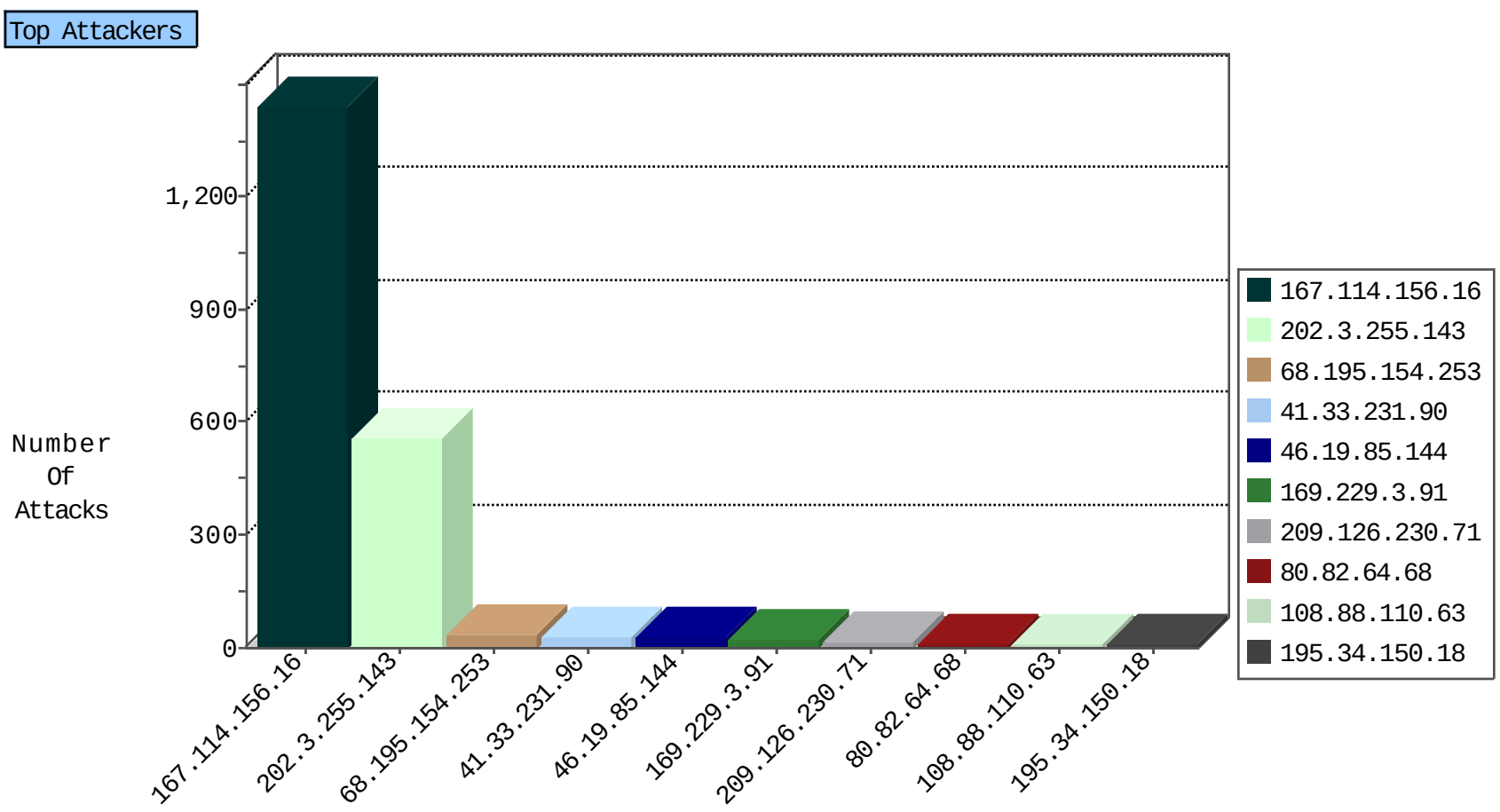
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-18-2016-03:04:00 to 01-18-2016-04:04:00

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	3000
123.151.149.222	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
89.248.174.4	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

01-18-2016-03:04:00 to 01-18-2016-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-18-2016-03:04:00 to 01-18-2016-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	519
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
66.249.78.79	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
191.179.226.157	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.71	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.34	Kazakstan	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
204.151.244.17	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

01-18-2016-03:04:00 to 01-18-2016-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
46.19.85.144	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.144	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
108.88.110.63	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
70.199.112.33	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
213.8.204.64	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
199.30.24.153	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
209.126.230.71	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
209.126.230.71	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
89.108.144.114	Lebanon	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
217.132.41.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
171.96.167.248	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.255.215.87	France	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	2
184.105.139.102	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.82	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.80	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.216.131	Netherlands	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.196	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.192	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.230.71	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
107.142.145.4	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.106	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.87	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.230.71	United States	147.237.0.33	idf.il	drop		drop	1
128.232.110.28	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.192	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.230.71	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.106	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.88	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.230.71	United States	147.237.0.35	akaws.idf.il	drop		drop	1
128.232.110.28	United Kingdom	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.154.146.225	France	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
157.56.0.165	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.192	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
119.140.202.86	China	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method Â¬[[#0]][[#0]][[#0]]AÂ¢	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.159	Israel	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	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL [[#24]]Ãœ×škn_9Â¯Ãž woe[[#23]]×?xÖ±×špq×˜×¥	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to qassam.ps/files/martyrs/37ee9280da.jpg	Block	1
209.126.230.71	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method b;JÂ ÃžÃ€7Ã€Â?Â¹>Â Â?Ã„ Âµ_Â¦Ã†Ã±Â¼([[[#1]]Ã,Ã,bÃ°Ã´Ã¿ÃªÂž[[#31]]vÂ”@Ã…	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
5.39.216.131	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
141.212.122.81	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /x	Block	1
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
207.46.13.24	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.24	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsit	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Distributed Malformed URL	Block	1
209.126.230.71	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1
91.109.247.173	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	1
157.55.39.224	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
68.195.154.253	United States	147.237.76.42	refuah.idf.il	NULL Character in Method Â¬[[#0]][[#0]][[#0]]AÂ¢	Block	1
207.46.13.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/..aspx	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Distributed Unknown HTTP Request Method	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
91.109.247.173	United Kingdom	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	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method b;JÂ ÃžÃ€7Ã€Â?Â¹>Â Â?Ã„Âµ_Â¦Ã†Ã±Â¼([[[#1]]Ã,Ã,bÃ°Ã´Ã¿ÃªÂž[[#31]]vÂ”@Ã… in URL	Block	1
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.73.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	1
157.55.39.230	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
207.46.13.94	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
188.138.1.218	Germany	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15344-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Query String on [[#24]]Ãœ×škn_9Â¯Ãž woe[[#23]]×?xÖ±×špq×˜×¥	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	1
68.195.154.253	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Â¬[[#0]][[#0]][[#0]]AÂ¢ in URL	Block	1
207.46.13.189	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1