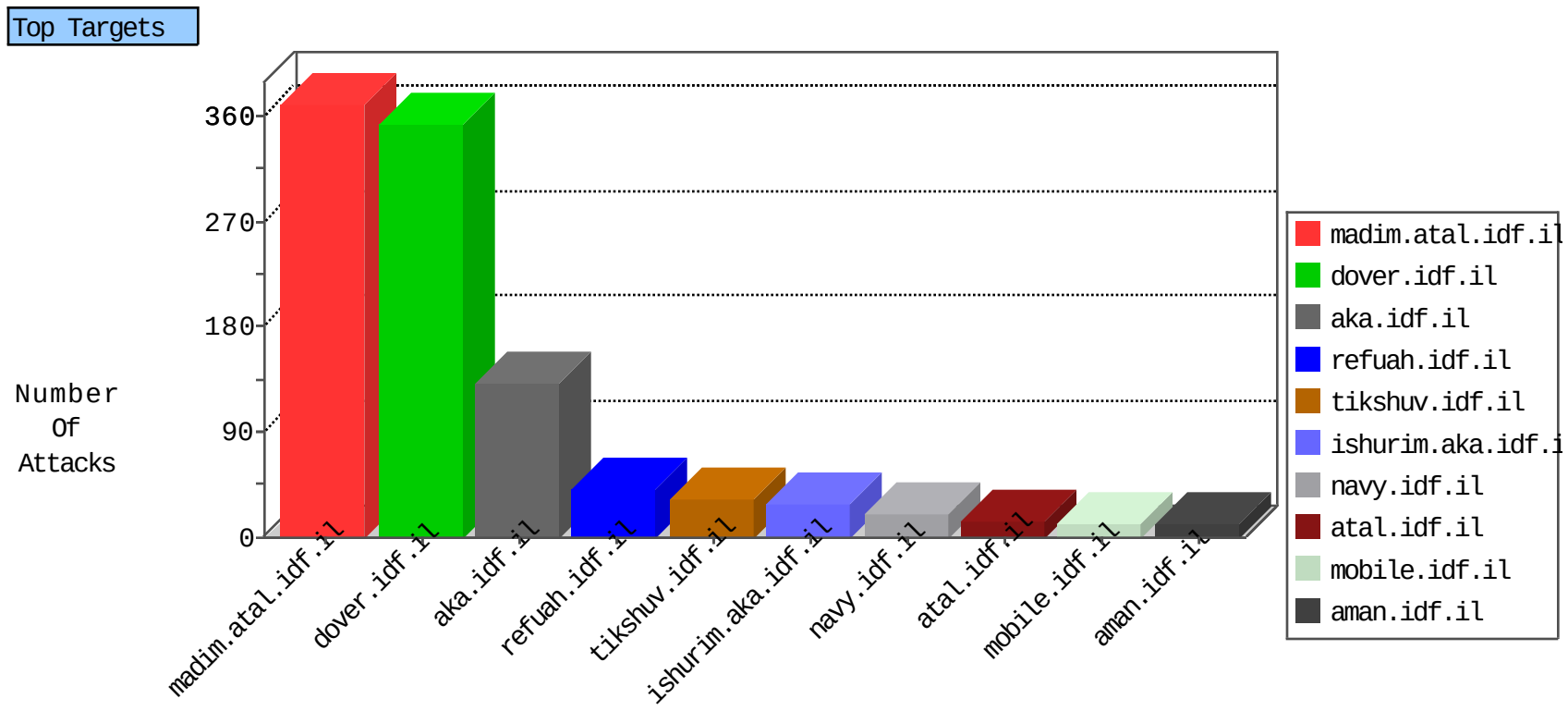
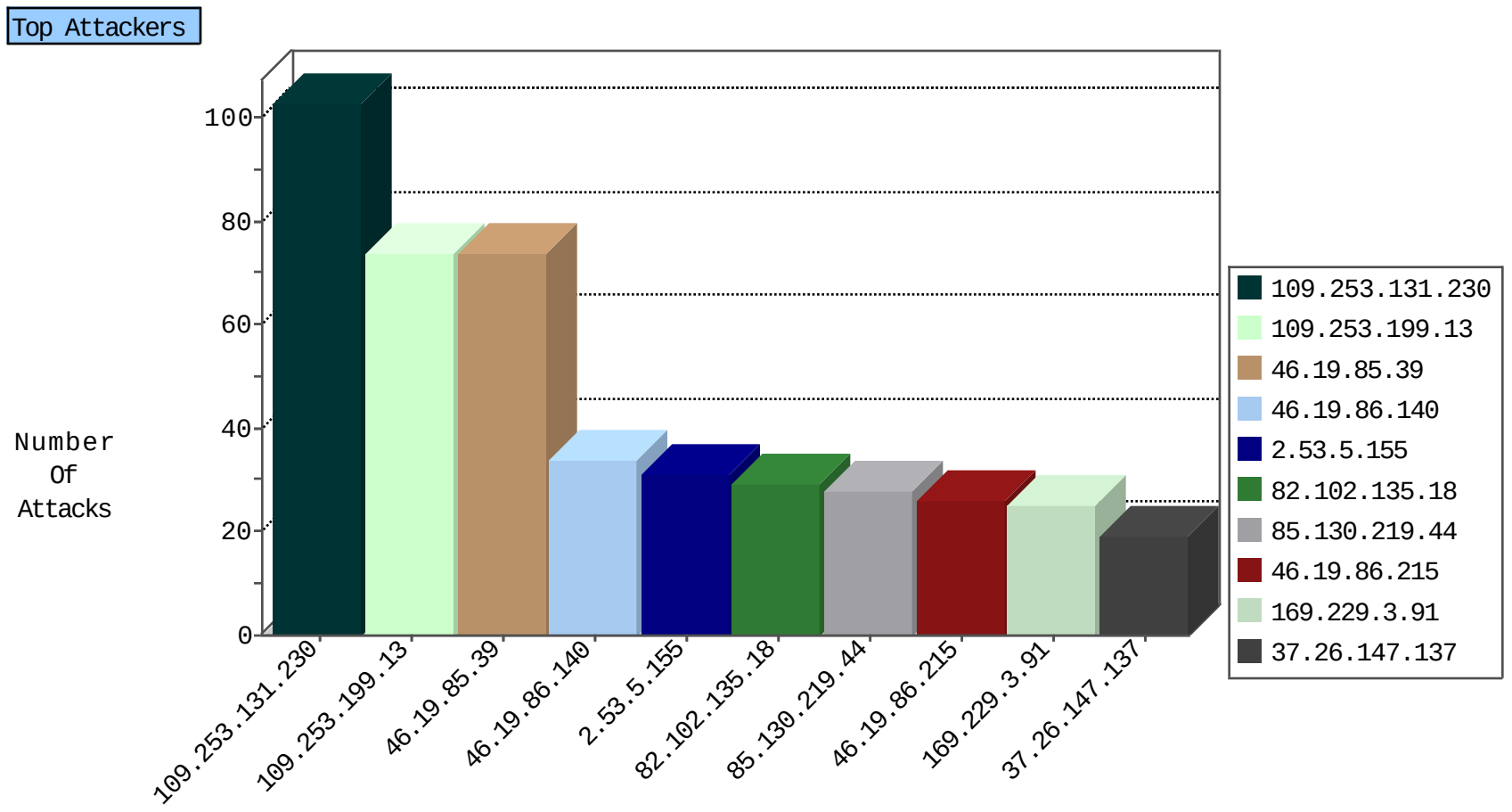
09-21-2016-12:04:03 to 09-21-2016-13:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-12:04:03 to 09-21-2016-13:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.199.17	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
82.81.57.4	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
89.138.182.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
80.246.138.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
80.246.138.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
176.13.246.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
141.226.161.83	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.32.179.214	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
141.226.146.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
85.64.144.209	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
209.126.136.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-21-2016-12:04:03 to 09-21-2016-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-21-2016-12:04:03 to 09-21-2016-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.235.60.218	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
211.149.244.79	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
31.210.187.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.207.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.65.82.44	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.135.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.144.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.57.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.44.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.8.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.61.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.170.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.241.137.4	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.83.162	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
121.46.87.116	147.237.77.216	India	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.138.182.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.188.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.39.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.120.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.101.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-21-2016-12:04:03 to 09-21-2016-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.102.135.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.86.215	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	24
185.137.19.158		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.140	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
80.246.139.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
37.26.147.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.130.219.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.21	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
141.226.161.78	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.12.160.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.219.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
62.0.212.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
85.130.219.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.147.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
85.64.17.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.71.1.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.248	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.164	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.130.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.246.136.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.224.129	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
2.53.10.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.182.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
62.219.13.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.22.134.89	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.254.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.138.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.65.254.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.55.143.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.234.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.140	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.140	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
111.93.113.149	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.140	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.254.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.161.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.92.136.11		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.201	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.139.39.51	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.143.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-21-2016-12:04:03 to 09-21-2016-13:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.131.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
109.253.199.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
2.53.5.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
80.246.137.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.135.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.228.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
37.26.147.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.55.147.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
213.57.243.74	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	8
185.32.179.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.132.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.187.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
109.253.221.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	3
109.253.140.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.135.244	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	2
192.117.158.212	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/205-he/patzar.aspx	Block	2
109.253.159.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.160.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.174.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
111.93.113.149	India	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	2
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza>специальном сайте , созданном для этих целей. <table cellspacing=	Block	1
46.19.85.0	Israel	147.237.76.31	nakchal.idf.il	Distributed Malformed URL	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.115.177.202	Block	1
79.181.58.186	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
62.176.77.100	Bulgaria	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method [[#1]]k[[#25]][[#16]]LG•~zõ0xþ”æï[[#1]]M[[#26]]ƒQþfc®2ŠKÁo”ÄÖ2 in URL	Block	1
152.62.109.205	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 209.88.198.1	Block	1
109.64.56.239	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name	Block	1
46.19.85.0	Israel	147.237.76.31	nakchal.idf.il	Distributed Unknown HTTP Request Method	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method w[[#21]]éŸÿšJëtø{Âˆê[[#22]]`í‘>qöàÿS•â(«ŠwõÉ*Ò?ï'6Í=5oã+M’ in URL	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method Ìü[[#1]]õˆrÏÆšLüÂ3[[#3]]þ in URL	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
66.102.6.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
157.55.39.11	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
37.26.147.198	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.13.245.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.194.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method °Wï6âuÞ[[#14]]E[[#28]]èº0¨[[#16]]ÉjâëK[	Block	1
77.138.245.247	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
46.19.85.0	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version _pk_ses.119.2366=*	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1

09-21-2016-12:04:03 to 09-21-2016-13:04:03