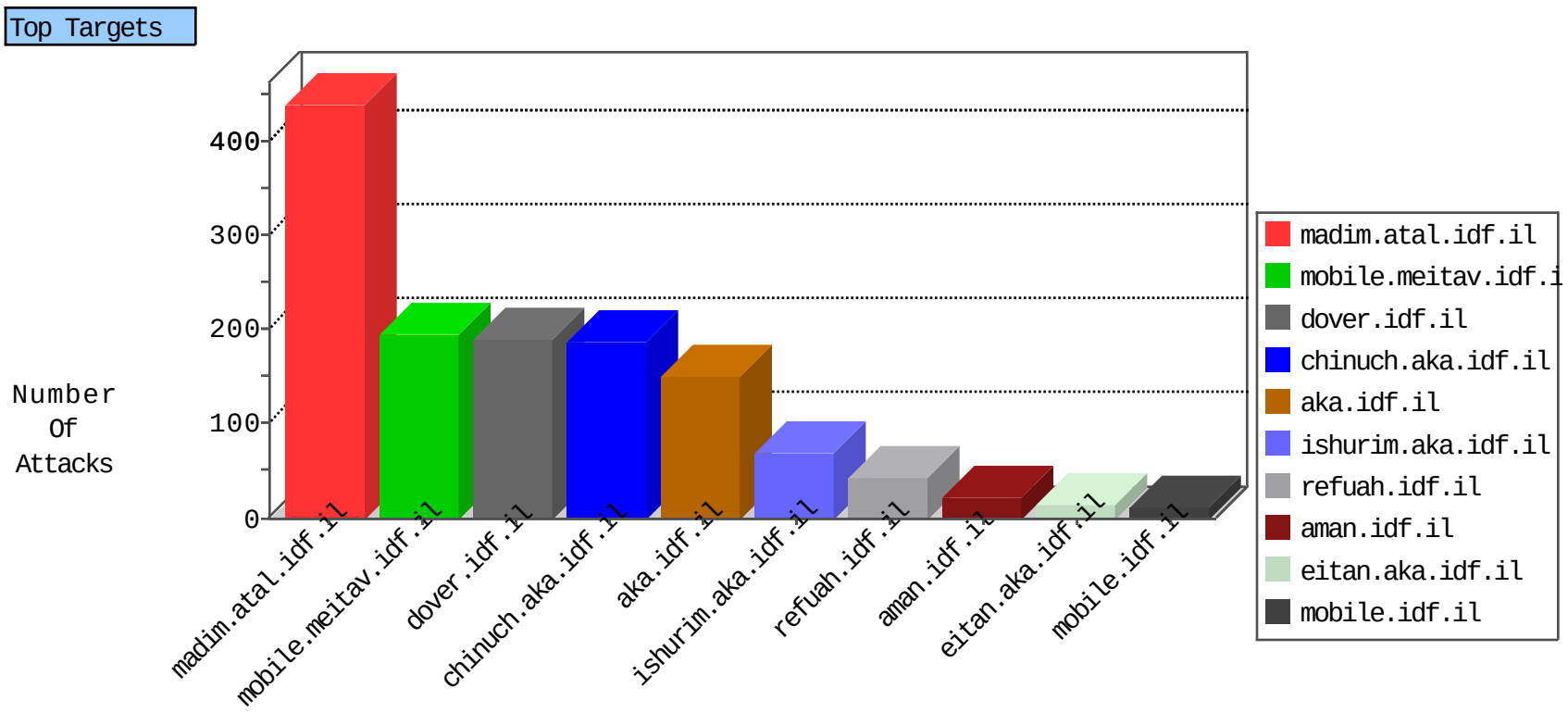
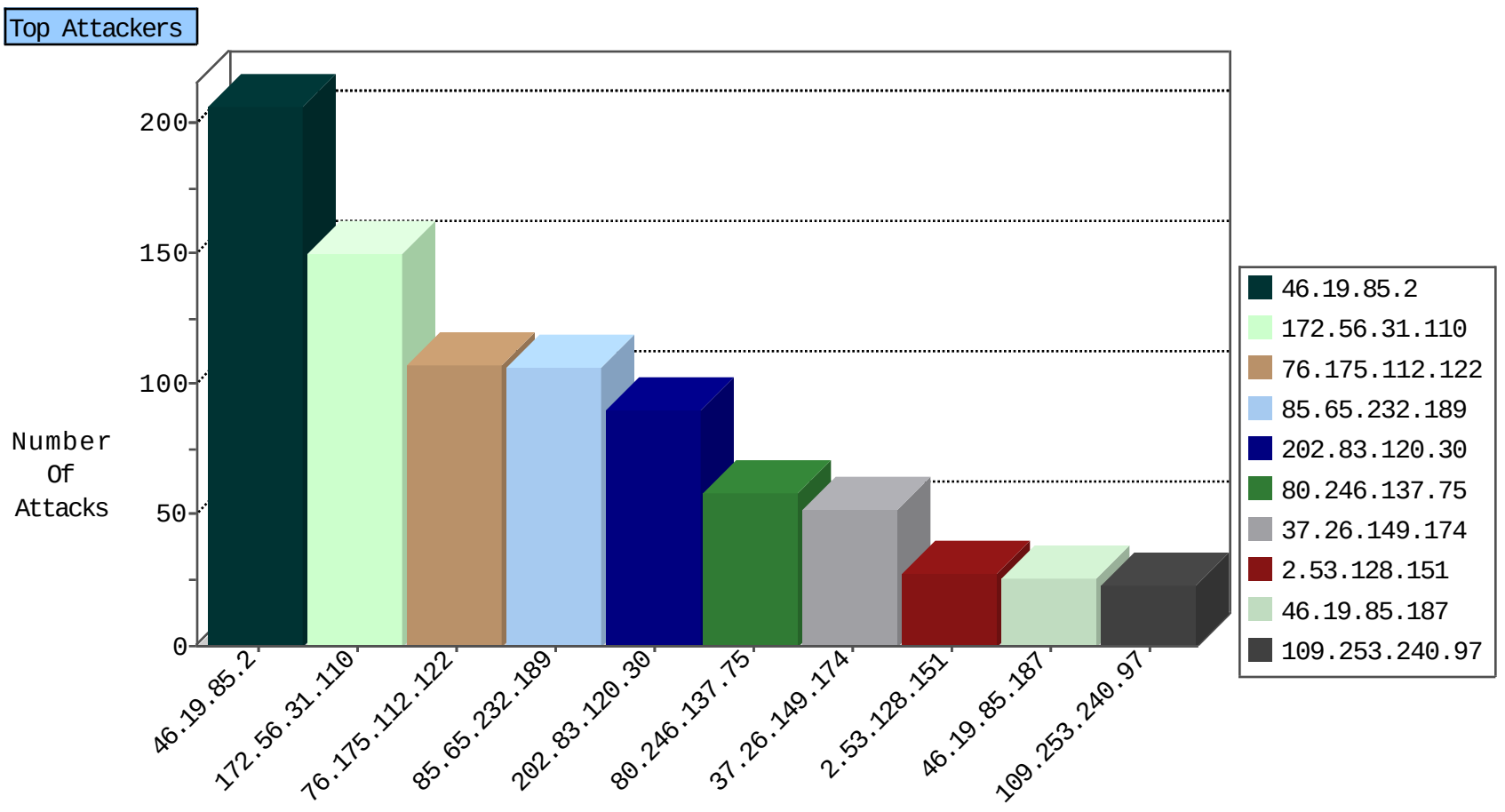
09-25-2016-12:04:01 to 09-25-2016-13:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-25-2016-12:04:01 to 09-25-2016-13:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.98.84	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
37.46.41.243	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	3
46.116.45.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
191.96.249.34	Chile	147.237.76.42	refuah.idf.il	Black List	drop	1

09-25-2016-12:04:01 to 09-25-2016-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-25-2016-12:04:01 to 09-25-2016-13:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.53.14.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.145.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.238.140.131	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.135.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.212.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN Potential SSH Scan	1
62.219.233.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
62.90.72.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.117.241.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.19.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.149.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.173.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.94.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.16.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.238.140.131	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
82.81.142.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.238.140.131	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
79.182.136.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
77.138.29.16	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
62.219.120.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
176.13.20.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.164.44	147.237.72.217	Romania	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.102.254.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.119.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.186.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-25-2016-12:04:01 to 09-25-2016-13:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
172.56.31.110	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	81
172.56.31.110	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	69
76.175.112.122	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	56
76.175.112.122	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	52
177.23.177.146	Brazil	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	18
37.26.149.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	18
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	12
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
37.26.149.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.192.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	9
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.199.71.118	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.204	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.235	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.237.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
62.0.211.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
202.83.120.30	Indonesia	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.53.128.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.164.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.151.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.148.238	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
37.26.149.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.149.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	alert	5
199.203.93.50	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
199.203.93.50	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.177	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.223.31.122	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
192.223.31.122	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.223.31.122	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.154.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.33.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
202.83.120.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.174	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		alert	4
2.53.151.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.55.18.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-25-2016-12:04:01 to 09-25-2016-13:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	207
85.65.232.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
80.246.137.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
109.253.240.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.53.128.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
212.76.107.109	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	13
188.120.135.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	11
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.212.165	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.212.165	Block	3
176.13.0.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.23.193	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
2.53.158.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.85.241	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/	Block	2
2.53.57.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.232	Block	2
46.19.85.83	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
109.253.193.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.212.22	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1331-he/refuah.aspx	Block	2
176.13.245.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.181.156	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
2.55.173.91	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
109.66.6.33	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in URL \kd(•`[[ע‰ת#17xŸ]]ıı›¥b: ¦~¼)7¯g;*	Block	1
79.178.23.193	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	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
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
109.253.192.43	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL \kd(•`[[ע‰ת#17xŸ]]ıı*;g¯7)¼~¦›¥b:	Block	1
207.46.13.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
54.210.231.197	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/web-console/serverinfo.jsp	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
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
77.139.212.165	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
176.13.14.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/userdetails	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2412.jpg	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
2.53.156.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.108.44	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1

09-25-2016-12:04:01 to 09-25-2016-13:04:01