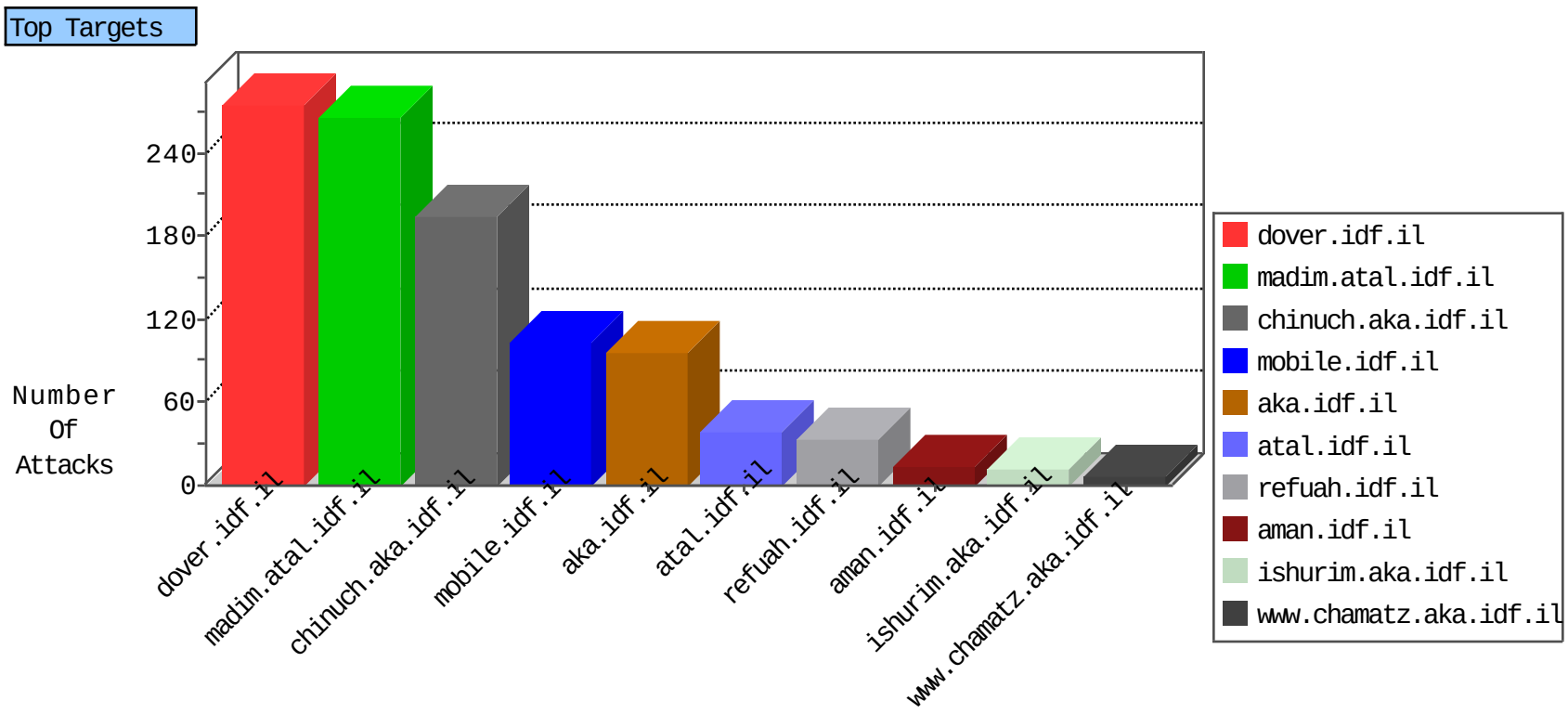
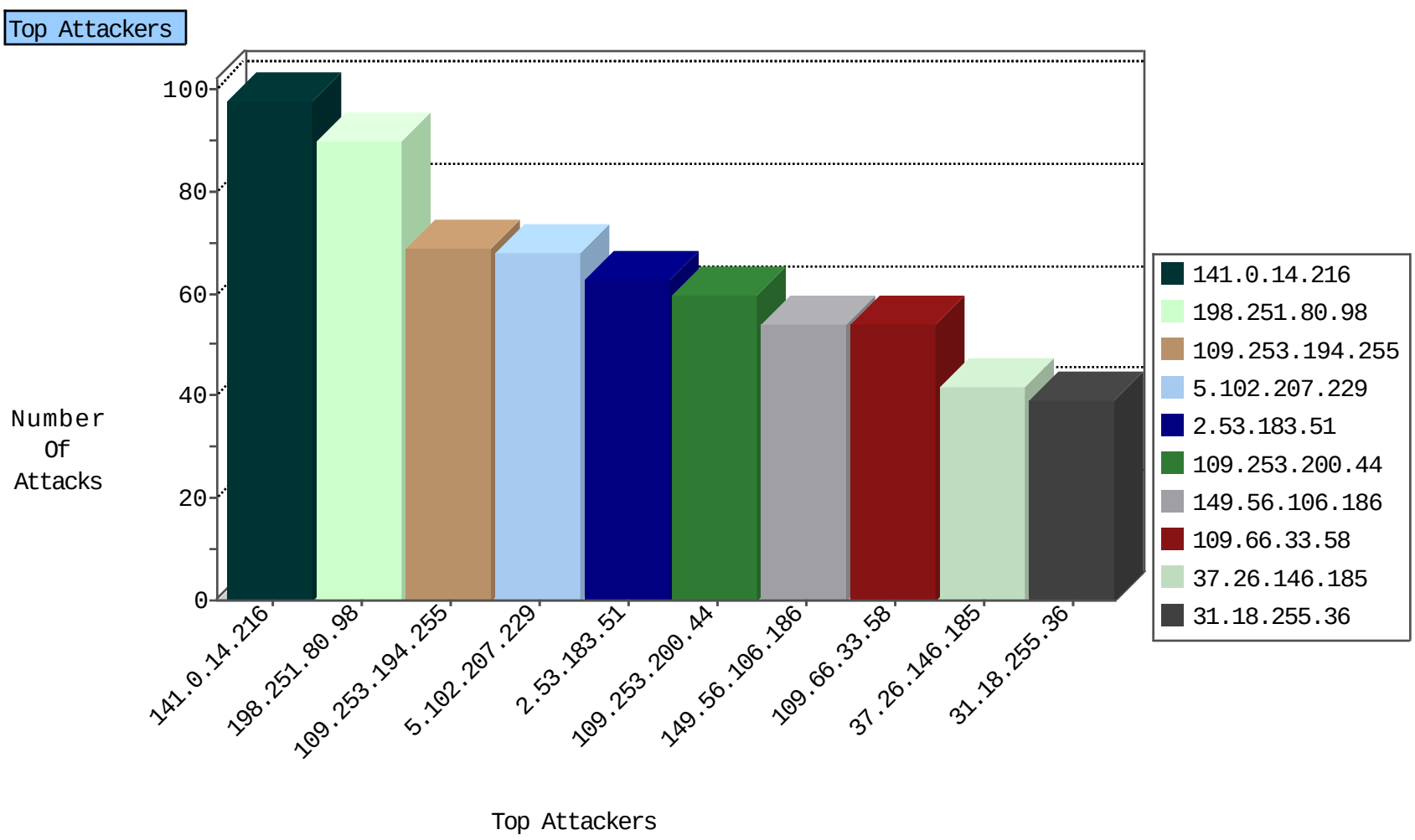
09-24-2016-21:04:04 to 09-24-2016-22:04:04

IDF Under Attack Daily Report



Top Target



Top Attackers

09-24-2016-21:04:04 to 09-24-2016-22:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.29.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.i	Black List	drop	1
71.6.146.185	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-24-2016-21:04:04 to 09-24-2016-22:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
51.254.131.243	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
95.91.45.174	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-24-2016-21:04:04 to 09-24-2016-22:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.87.109.253	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
220.169.242.158	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
211.149.197.148	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
195.143.227.35	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.229.172.116	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.169.242.158	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
220.169.242.158	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
220.169.242.158	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.143.227.35	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
218.87.109.253	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
125.77.28.26	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.229.172.116	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
221.229.172.116	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.210	147.237.76.30	Europe	himush.idf.il	ET SCAN NMAP -sA (2)	1
218.87.109.253	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
31.154.81.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.169.242.158	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016-21:04:04 to 09-24-2016-22:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.216	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
109.66.33.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
31.18.255.36	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
141.0.14.216	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	32
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
77.126.94.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.56.106.186	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
149.56.106.186	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
149.56.106.186	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
37.26.146.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
37.26.146.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
37.26.146.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
193.5.216.100	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
89.237.121.61	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.116.44.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
149.56.106.186	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
89.237.121.61	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.139.108.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.240.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.120.125.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
80.246.130.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.219.130.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.55.168.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.56.106.186	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
197.159.205.200	Cote D'Ivoire	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.185	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
80.179.109.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.76	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.116.44.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.148.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.235.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.194.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
5.102.207.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
2.53.183.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
79.176.143.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.53.63.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.116.117.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
188.120.154.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	5
84.229.73.143	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.117.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/2/	Block	3
79.177.3.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.104.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.192.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2808.jpg	Block	1
99.237.65.43	Canada	147.237.72.166	aka.idf.il	Unknown Parameter CatId in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.93.158	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	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
2.55.55.253	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.66.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/5/245.doc	Block	1
46.19.85.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.153	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
87.68.0.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
5.22.134.185	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.27	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/3/243.doc	Block	1
157.55.39.160	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
89.132.235.64	Hungary	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.160.255.199	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	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
79.178.118.11	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9031-he/refuah.aspx	Block	1
99.237.65.43	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspxcatid=58604	Block	1
2.53.158.121	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
66.249.93.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
82.81.100.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/guiys	Block	1

09-24-2016-21:04:04 to 09-24-2016-22:04:04