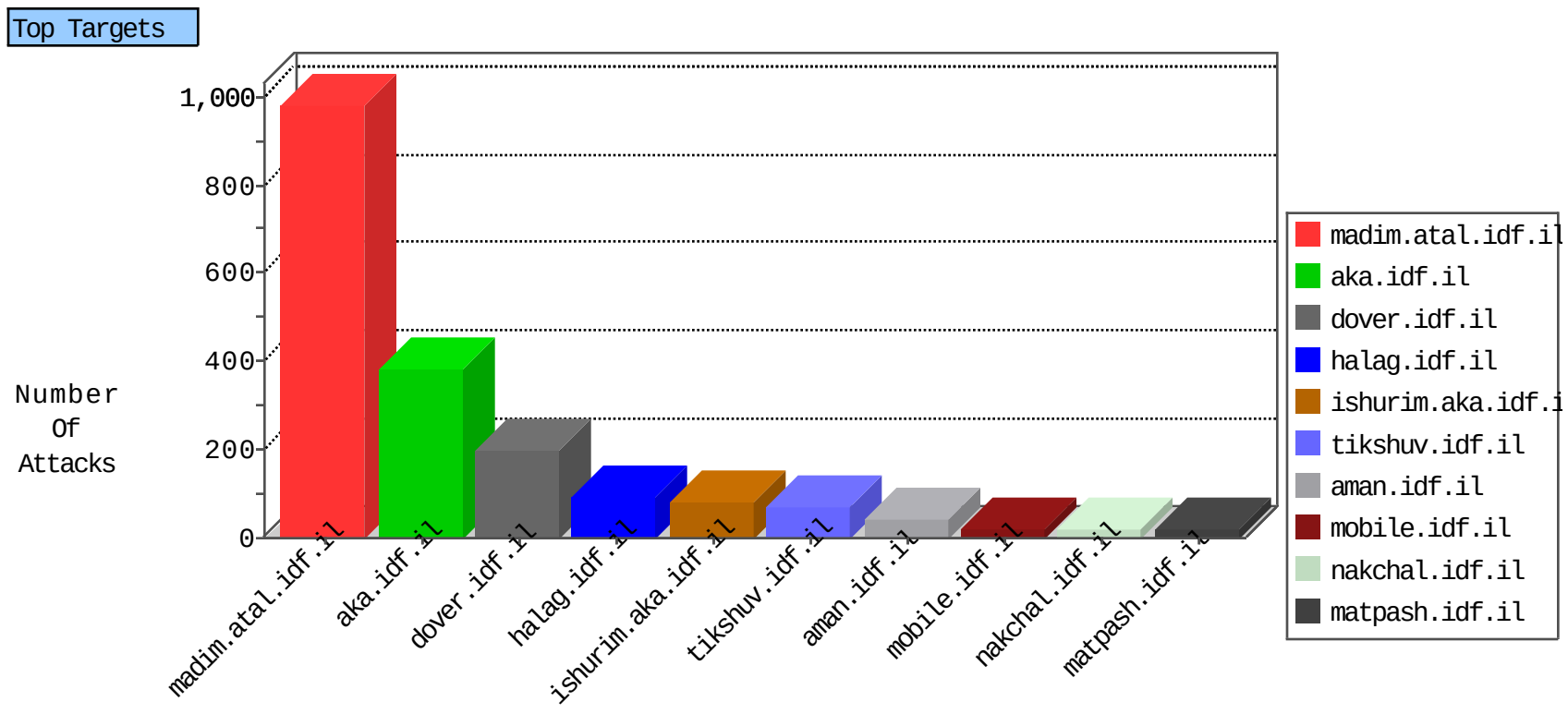
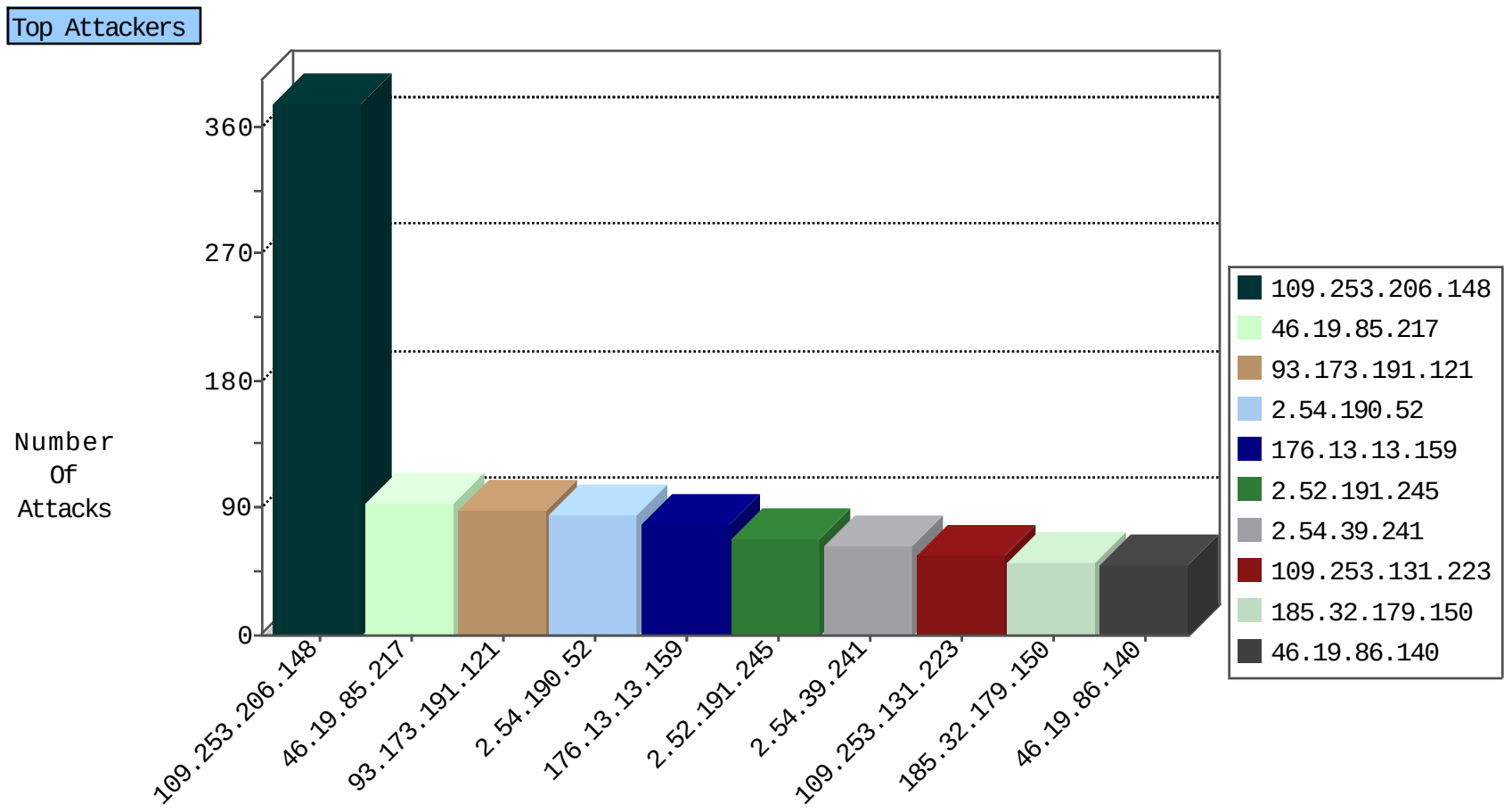
01-27-2016-12:04:05 to 01-27-2016-13:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-27-2016-12:04:05 to 01-27-2016-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.195.231	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
61.182.170.38	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

01-27-2016-12:04:05 to 01-27-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-27-2016-12:04:05 to 01-27-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.110.85.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.111.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.9	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
31.210.187.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.117.121.60	147.237.77.170	Korea, Republic of	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
193.124.249.104	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.154.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.228.112	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
54.179.135.126	147.237.72.167	Singapore	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
212.179.46.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.117.121.60	147.237.77.170	Korea, Republic of	maarachot.idf.il	ET SCAN NMAP -f -sS	1
194.90.25.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-27-2016-12:04:05 to 01-27-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.173.191.121	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	85
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
109.253.206.148	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
185.120.126.56		147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
37.26.146.214	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.61	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.61	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.213.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
109.253.213.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.149.143	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
2.52.138.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.132	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.7.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.187.50	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.17.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.151.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.10.156	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.182.209.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.201.1	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.129	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.132	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.201.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.101.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.68.74.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.85	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	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
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.244	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.85	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.3.147.151	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.187.50	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.102.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.121.99.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.175.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
80.246.137.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.17.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.187.50	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.187.50	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
220.161.117.11	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
109.253.206.148	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.17.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

01-27-2016-12:04:05 to 01-27-2016-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	203
109.253.206.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	139
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
2.54.190.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	85
176.13.13.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
2.52.191.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
109.253.131.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
185.32.179.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
46.19.86.140	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
2.54.39.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
80.246.136.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
176.13.22.128	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.13.22.128	Block	19
2.54.39.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
109.253.129.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
132.64.212.113	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	10
176.13.9.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
2.54.165.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.206.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	9
80.246.139.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.85.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.20.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
62.219.195.38	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	5
109.253.142.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.199.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.200.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.219.195.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
213.8.245.50	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.245.50	Block	3
2.54.180.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.82.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
108.62.19.210	United States	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 108.62.19.210	Block	2
212.179.226.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
79.178.181.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
108.62.19.210	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 108.62.19.210	Block	2
2.54.135.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.166.240.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
108.62.19.210	United States	147.237.72.166	aka.idf.il	Multiple Malformed URL from 108.62.19.210	Block	2
2.52.138.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.109.70.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/sachar/default.aspx	None	2
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
108.62.19.210	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 108.62.19.210	Block	1
108.62.19.210	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 14	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
176.13.20.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.191.121	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
109.64.174.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
212.150.203.146	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1

01-27-2016-12:04:05 to 01-27-2016-13:04:05