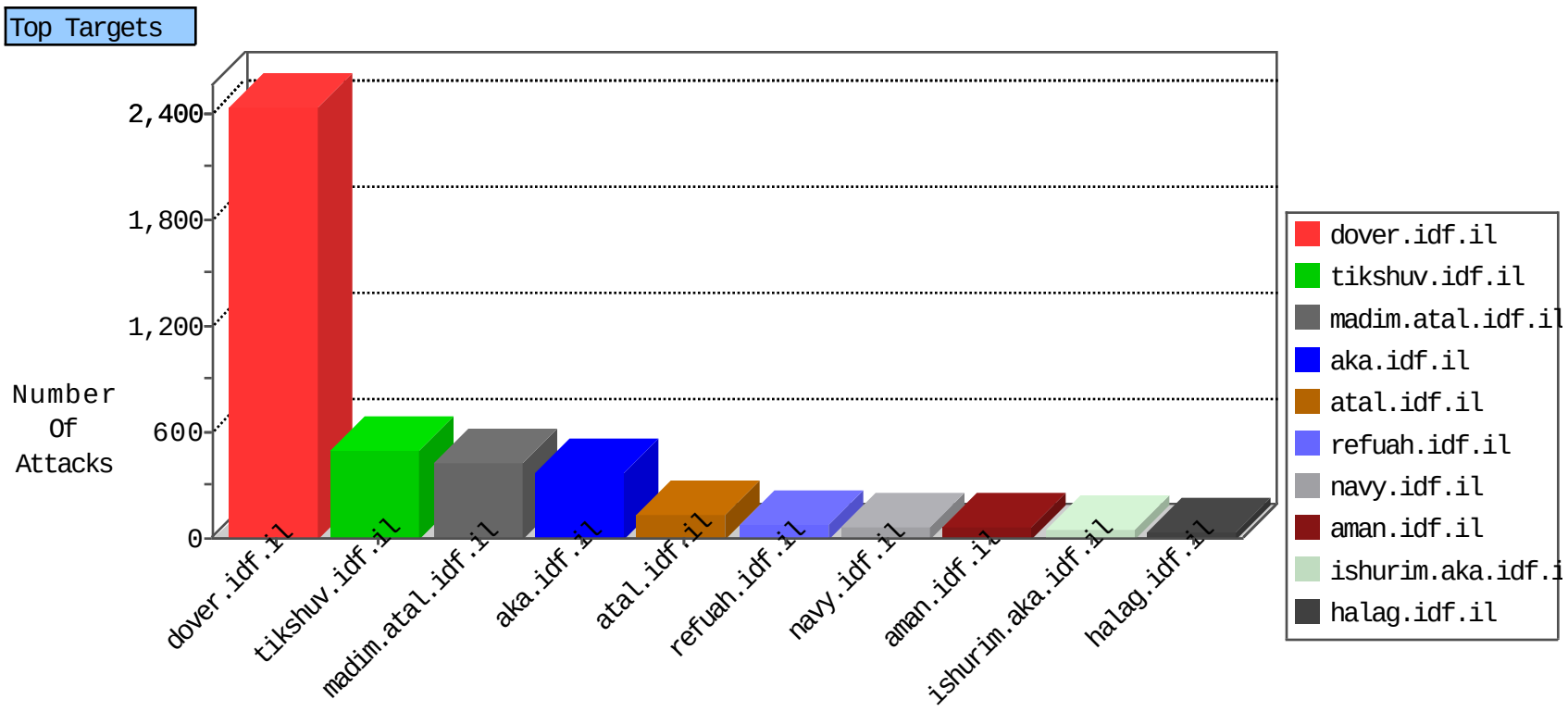
01-13-2016-15:04:08 to 01-13-2016-16:04:08

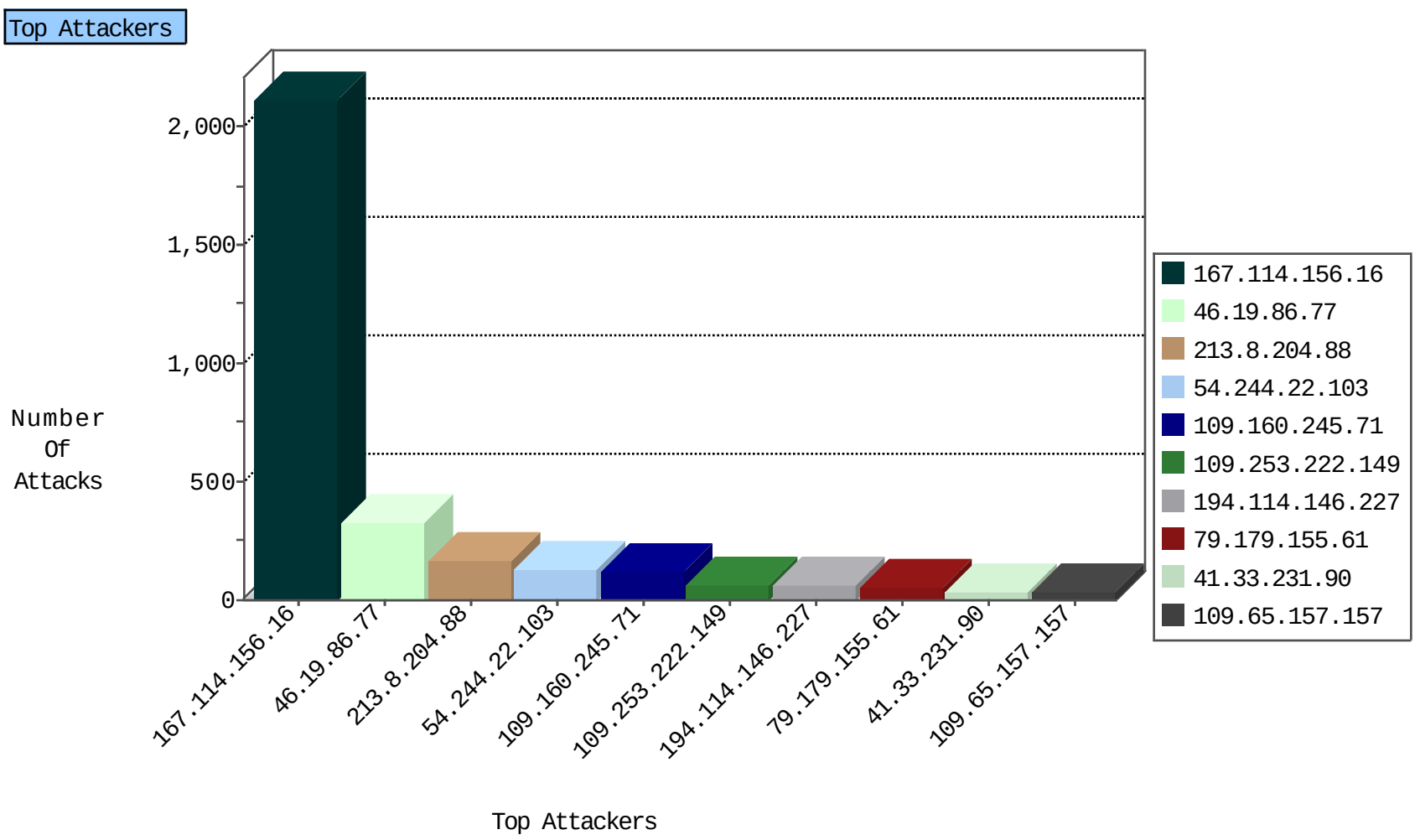
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-13-2016-15:04:08 to 01-13-2016-16:04:08

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	3231
84.111.13.84	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
31.13.160.217	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
183.60.48.25	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
63.141.227.98	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.211	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
63.141.227.98	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
63.141.227.98	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

01-13-2016-15:04:08 to 01-13-2016-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-13-2016-15:04:08 to 01-13-2016-16:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.29.247.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.128.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.229	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.247	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.64.232.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.118.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
158.255.6.220	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.12.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

01-13-2016-15:04:08 to 01-13-2016-16:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.65.157.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.86.128	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
37.26.146.155	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
5.29.247.44	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
110.159.188.251	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
80.246.130.89	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.0.101.97	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
79.181.28.243	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
62.0.101.97	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
62.219.115.30	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.86.16	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
185.120.126.44		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
185.120.126.44		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
62.219.133.179	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
172.56.19.237	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
54.244.22.103	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
54.244.22.103	United States	147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
188.161.107.114	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
185.89.217.234		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
109.65.157.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
147.235.8.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
147.235.8.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.253	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
147.235.8.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
31.210.188.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.6.17.44	Palestinian Territory Occupied	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.163	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.235.28.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
31.210.188.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.133.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.227		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.163	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.95	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.111.226.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	219
213.8.204.88	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	161
109.160.245.71	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	116
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
109.253.222.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
79.179.155.61	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
109.65.178.221	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
79.176.98.199	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	8
89.138.97.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main.sachar	Block	7
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.129.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
5.28.154.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.11.203	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
185.120.126.44		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
46.19.85.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.214.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.74	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.74	Block	2
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	2
5.28.154.60	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.66.206.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.138.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.211.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
199.207.253.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
2.54.177.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.221	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.11.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.28.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/newpassword/firstlogin	Block	1
79.180.49.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
202.142.119.135	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.27	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
109.65.157.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
192.115.248.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
37.26.148.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.121.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.35.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.156	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
80.82.64.68	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to habbo.yt/public/css/960_12_col.css	Block	1
207.46.13.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/12607.jpg	Block	1
109.201.152.21	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.142.68.30	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
95.35.37.153	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.176.103.156	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1

01-13-2016-15:04:08 to 01-13-2016-16:04:08