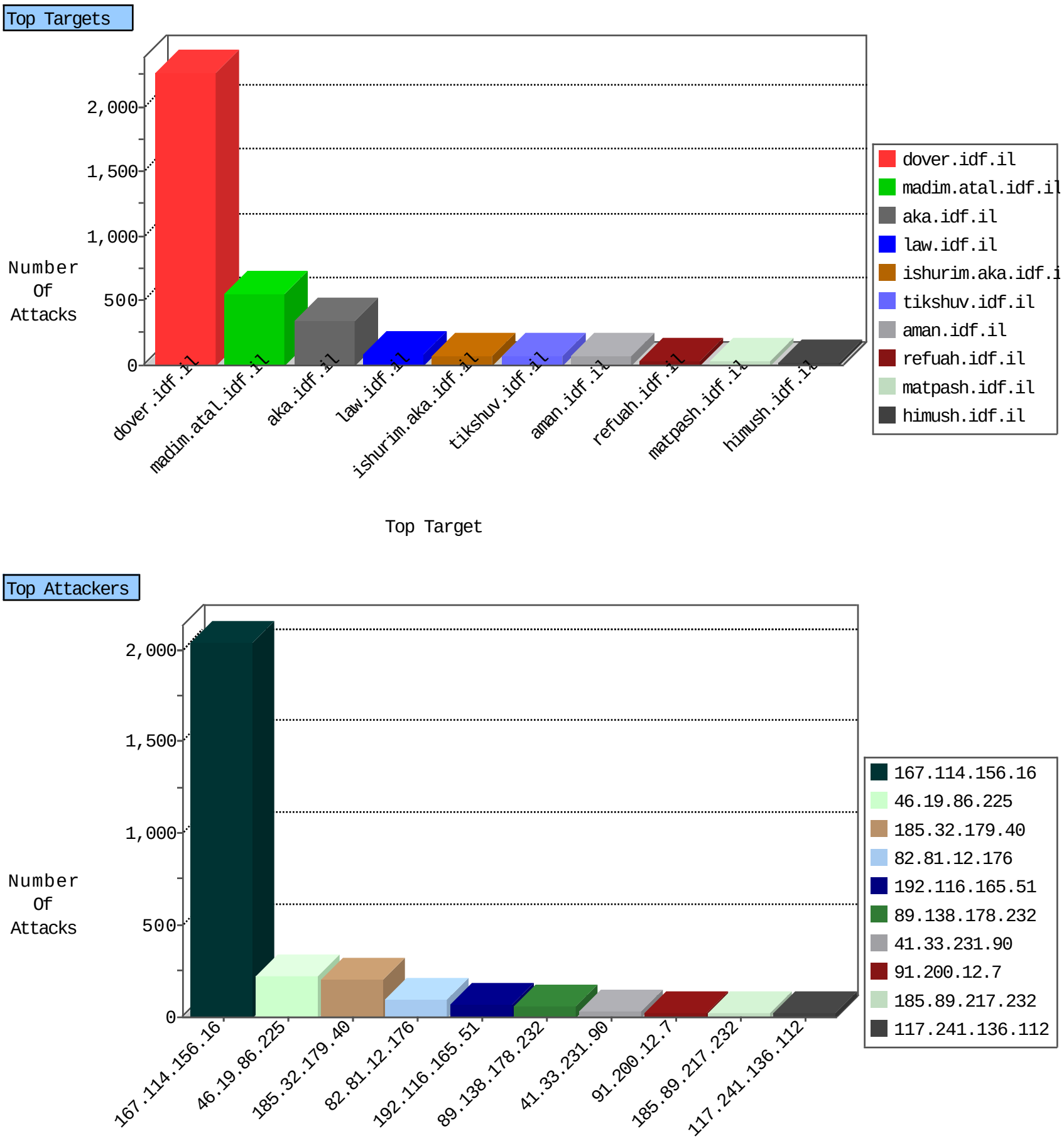
01-20-2016-09:04:07 to 01-20-2016-10:04:07

IDF Under Attack Daily Report



01-20-2016-09:04:07 to 01-20-2016-10:04:07

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	3196
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	96
84.108.85.95	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
194.89.24.49	Finland	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
89.248.168.218	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
194.89.24.49	Finland	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	1
93.88.67.168	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
89.248.168.218	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
89.248.168.218	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

01-20-2016-09:04:07 to 01-20-2016-10:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.132.209.23	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
88.229.145.165	Turkey	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
151.80.31.120	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
185.63.188.120	Russian Federation	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

01-20-2016-09:04:07 to 01-20-2016-10:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

01-20-2016-09:04:07 to 01-20-2016-10:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.116.165.51	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	67
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
50.117.45.90	Anonymous Proxy	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	20
79.180.190.23	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
185.89.217.231		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.232		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
109.253.200.234	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.13	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
82.80.64.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.20	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.200.234	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
91.186.242.37	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
154.99.252.56	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
154.99.252.56	Sudan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.225		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.105	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.126.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.228		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.150.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
117.241.136.112	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
154.99.252.56	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.54.30.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
117.241.136.112	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.12	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
117.241.136.112	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.46.39.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.54.7.233	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
117.241.136.112	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
194.89.24.50	Finland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.253.197.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.89.217.230		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.226		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.194.197.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.151.42.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.199.224.24	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	4
2.52.144.96	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.141	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

01-20-2016-09:04:07 to 01-20-2016-10:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
185.32.179.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	137
185.32.179.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
89.138.178.232	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 89.138.178.232	Block	36
89.138.178.232	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 89.138.178.232	Block	26
89.138.188.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.13.4.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.144.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
37.26.149.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	12
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.7	Block	11
81.218.70.243	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	8
37.26.148.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
89.139.237.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
64.71.32.27	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.71.32.27	Block	4
2.54.43.175	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
88.229.145.165	Turkey	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 88.229.145.165	Block	3
2.54.105.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.161.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
88.229.145.165	Turkey	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
185.32.179.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.199.224.24	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	2
2.54.138.47	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.21.167	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
37.26.149.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
88.229.145.165	Turkey	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
80.246.139.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.230.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.151.41.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/forms.aspx&sa=u&ved=0ahukewjn34wh8lfkahxitxqkhd3pboyqfggimaa&usg=afqjcngw-11fiu_bech3ic8tmplmgnpdta	Block	1
79.179.197.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.167.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.197.7	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/109070.pdf	Block	1
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.25.102.57	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.54.160.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.15.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/111340.pdf	Block	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 40.77.167.82	Block	1
216.218.206.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
2.54.173.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.64.184.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1

01-20-2016-09:04:07 to 01-20-2016-10:04:07