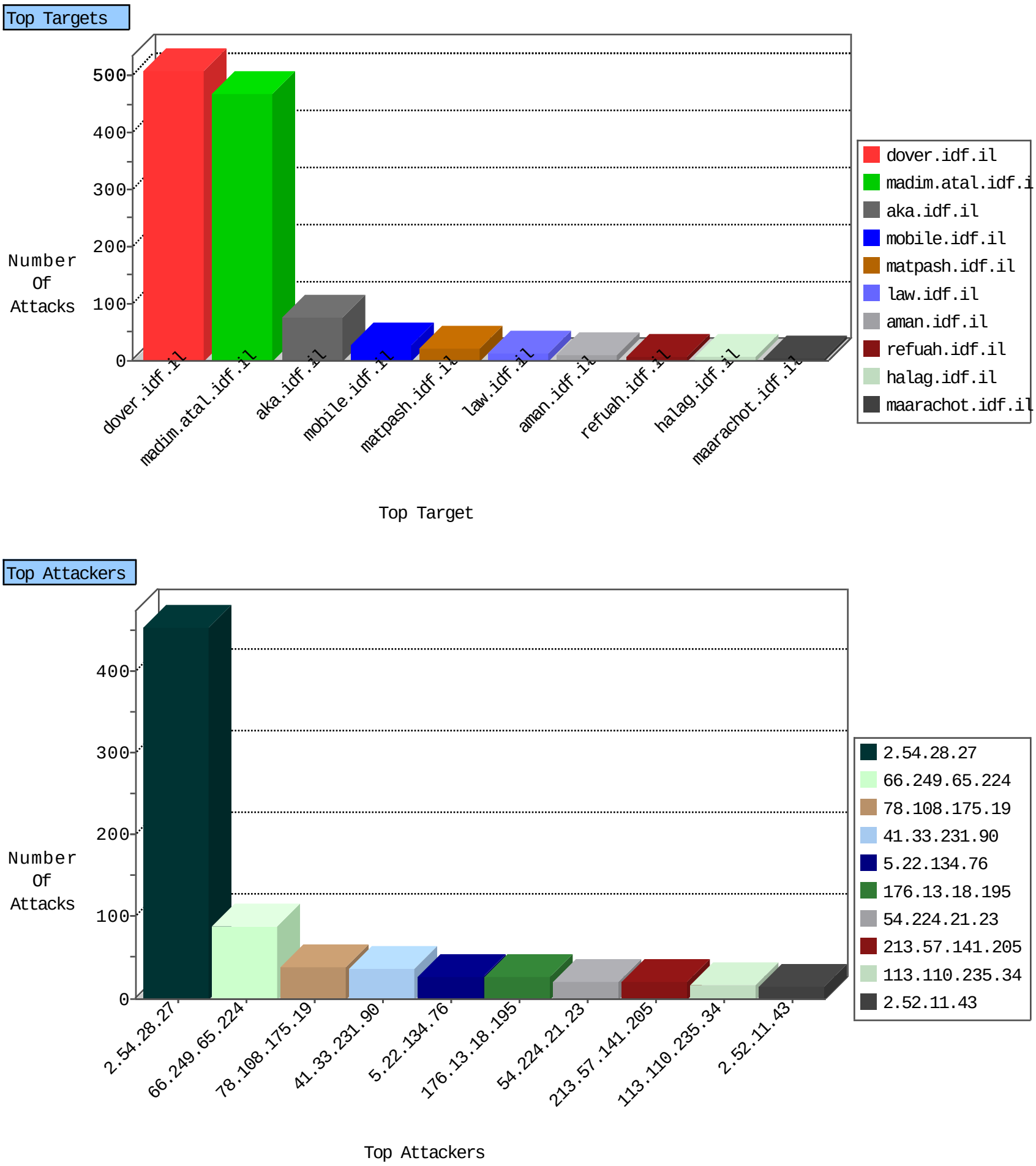
11-21-2015-00:04:09 to 11-21-2015-01:04:09

IDF Under Attack
Daily Report



11-21-2015-00:04:09 to 11-21-2015-01:04:09

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	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.228.97.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
89.179.73.99	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
86.133.244.252	United Kingdom	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

11-21-2015-00:04:09 to 11-21-2015-01:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.26.128.17	Romania	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	4

11-21-2015-00:04:09 to 11-21-2015-01:04:09

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	4
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
109.251.56.171	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
86.47.124.182	147.237.8.50	Ireland	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
50.18.225.195	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
185.106.94.57	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
23.99.54.247	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
182.23.51.250	147.237.0.35	Indonesia	akaws.idf.il	ET SCAN Potential SSH Scan	1
182.23.51.250	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
163.204.90.6	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.8.93.183	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.251.56.171	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
86.47.124.182	147.237.8.50	Ireland	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
54.176.4.242	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
31.6.71.154	147.237.0.19	Poland	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
182.23.51.250	147.237.0.200	Indonesia	m4u.idf.il	ET SCAN Potential SSH Scan	1
23.99.54.247	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
182.23.51.250	147.237.0.33	Indonesia	idf.il	ET SCAN Potential SSH Scan	1
182.23.51.250	147.237.0.16	Indonesia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
159.8.93.183	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1

11-21-2015-00:04:09 to 11-21-2015-01:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
78.108.175.19	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
5.22.134.76	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
176.13.18.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.52.11.43	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
189.224.130.170	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
113.110.235.34	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
213.57.141.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
213.57.141.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
82.102.222.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.160.21	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.67.122	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.141.26	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.34.76.178	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.16.156.125	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
41.232.153.241	Egypt	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
95.108.158.239	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.32.246.43	Italy	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
207.46.13.74	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.250.211.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.16.156.126	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
37.140.141.32	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.108.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
203.133.170.89	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.2.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.99.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.145.218.192	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
113.110.235.34	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
199.16.156.124	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
79.181.62.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
37.26.148.182	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
213.57.157.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

11-21-2015-00:04:09 to 11-21-2015-01:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.28.27	Block	230
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.28.27	Block	116
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
93.172.13.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
84.228.178.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.166.190.135	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
185.32.179.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.157.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.5.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
2.54.1.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.177.37.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
109.201.154.238	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.186.228.60	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
204.93.154.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on /	Block	1
171.25.193.25	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.177.58.76	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/	Block	1
185.3.146.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19550-he/dover.aspx	Block	1
113.110.235.34	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
40.77.167.15	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9235-he/refuah.aspx	Block	1
204.93.154.211	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
171.25.193.132	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/targilkakatz17042011.aspx	Block	1
109.65.8.73	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
79.177.191.13	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/6/size338x0/1686.jpg	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1159-he/chinuch.aspx	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
141.212.122.160	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
95.130.11.147	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
41.143.136.199	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.13.0.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl71 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/theunloadingofhumanitarianaidfromtheflotillacontinues.aspx	Block	1
109.201.152.250	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3192.pdf	Block	1
79.180.217.131	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
188.26.128.17	Romania	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

11-21-2015-00:04:09 to 11-21-2015-01:04:09