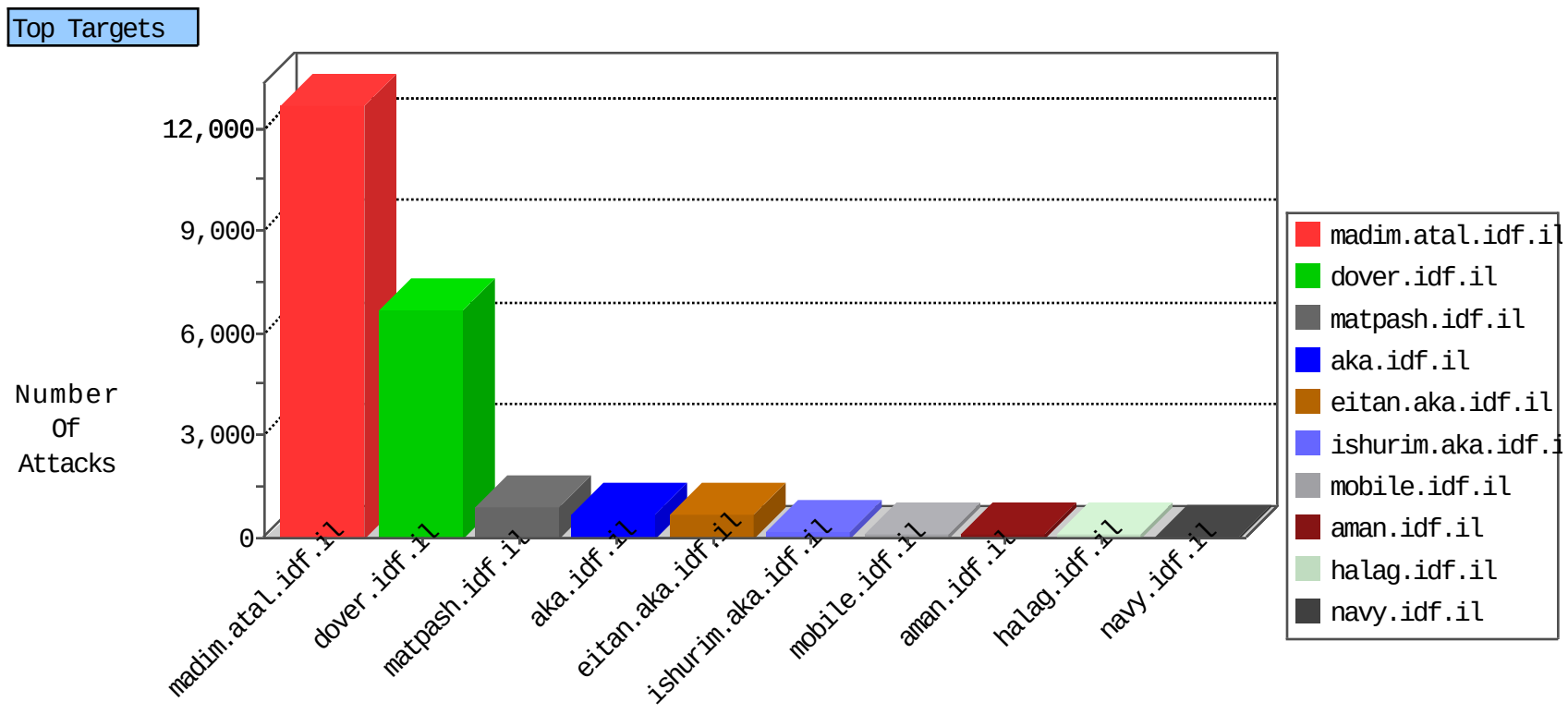
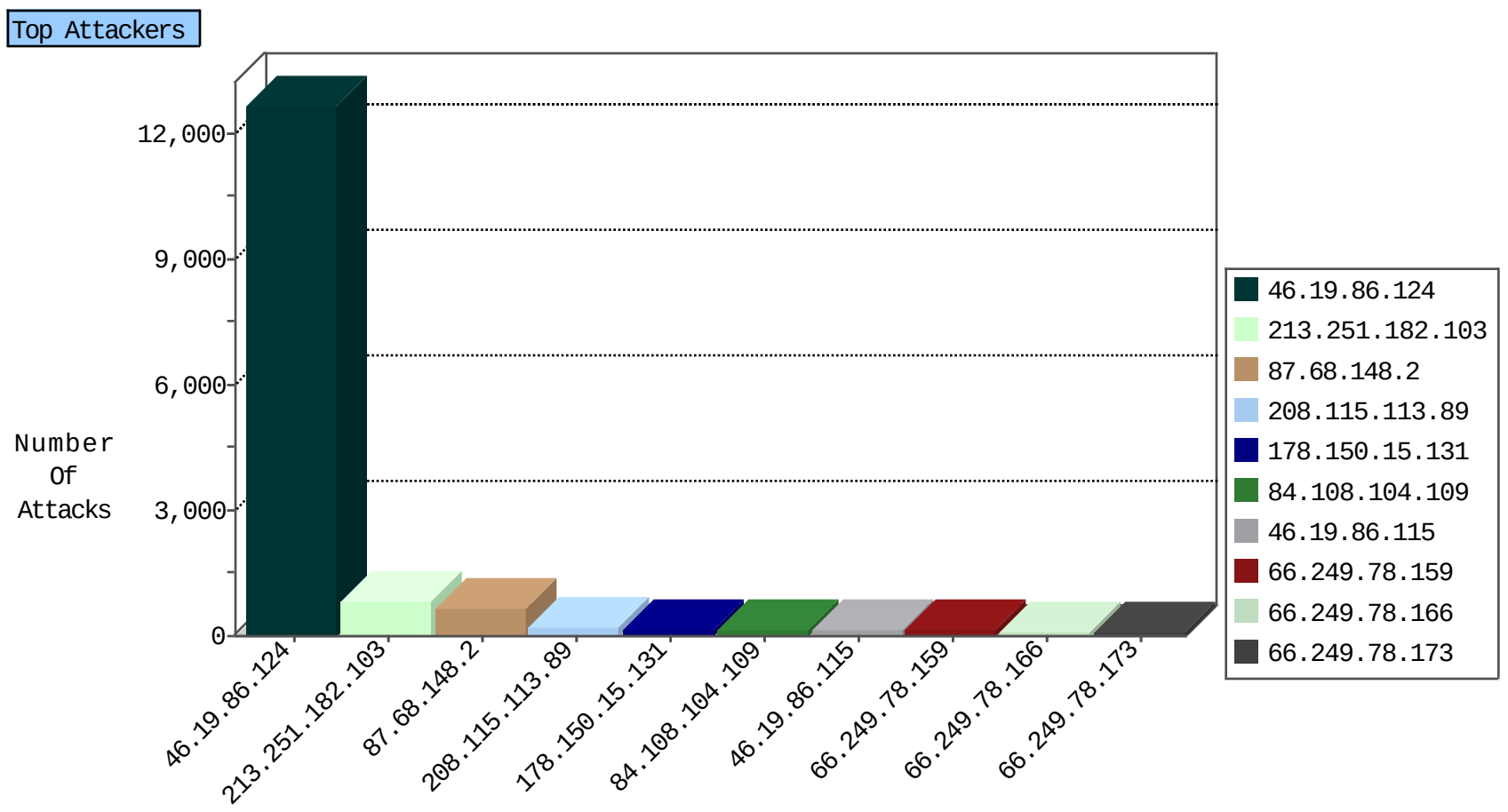
10-22-2015-20:04:06 to 10-22-2015-21:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-22-2015-20:04:06 to 10-22-2015-21:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	406
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	178
31.168.203.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	73
80.12.63.185	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	42
85.65.244.190	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	40
109.186.51.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	32
95.86.110.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.177.214.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
82.166.101.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
46.19.85.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
176.12.143.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
79.182.181.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
185.32.179.8	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
31.175.23.28	Poland	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
109.67.27.23	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
5.22.129.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
89.133.36.240	Hungary	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
50.159.6.225	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
89.138.221.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
85.64.1.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.136.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.57.12.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.186.185.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.57.210.126	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.228.199.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.111.100.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
174.102.139.58	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
89.138.226.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.228.19.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.117.158.93	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.65.215.220	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
179.158.82.203	Brazil	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.22.129.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
149.88.229.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
88.8.175.150	Spain	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
94.159.183.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.148.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
80.12.63.185	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.13.12.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
85.250.2.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.19.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
5.28.187.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
77.126.165.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.142.144.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.177.102.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
149.78.50.51	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
62.90.107.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

10-22-2015-20:04:06 to 10-22-2015-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
143.53.85.143	United Kingdom	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-22-2015-20:04:06 to 10-22-2015-21:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
27.75.168.255	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
27.75.168.255	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	4
80.246.136.179	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
221.228.67.62	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
183.87.125.98	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
182.48.105.216	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
176.13.23.66	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
93.173.35.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.148.20.22	147.237.77.226	Lithuania	www.chamatz.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
37.195.22.21	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.228.67.62	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.87.125.98	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
180.249.169.58	147.237.76.38	Indonesia	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.160.190.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.147.180.56	147.237.0.200	Saudi Arabia	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
221.228.67.62	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
37.195.22.21	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

10-22-2015-20:04:06 to 10-22-2015-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.68.148.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	372
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	180
84.108.104.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	148
46.19.86.115	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
5.28.177.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
199.249.227.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.19.85.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
50.159.6.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
82.166.101.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
46.19.86.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.196	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
89.138.199.205	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
88.8.175.150	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.116.161.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.78.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
37.142.116.214	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
37.142.115.206	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
149.88.229.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
198.103.184.76	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
109.67.60.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
80.12.63.185	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
31.154.157.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
179.158.82.203	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.85.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
76.173.132.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
79.177.151.122	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	29
213.244.65.138	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
37.201.193.2	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27

10-22-2015-20:04:06 to 10-22-2015-21:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.124	Block	12662
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	840
87.68.148.2	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	280
178.150.15.131	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	84
84.228.199.104	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	84
178.150.15.131	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.150.15.131	Block	70
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
79.179.191.113	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	28
31.154.157.231	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation searchText in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	26
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.110	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1120-he/nakhal.aspx	Block	14
89.139.24.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	14
188.143.232.16	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
142.54.172.110	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to dns.cloud.ph/	Block	14
85.250.65.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	14
157.55.39.126	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	14
89.234.68.70	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
84.94.179.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
212.150.209.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58607&docid=25004	Block	14
142.54.187.42	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on dns.cloud.ph/	Block	14
69.171.230.102	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	14
94.159.191.0	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
84.109.153.6	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
46.116.172.12	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	14
87.68.166.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
109.186.40.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mitgaisim	Block	14
84.228.97.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
50.159.6.225	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
87.69.134.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
77.125.97.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.19.85.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
178.150.15.131	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	14
142.54.172.106	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to dns.cloud.ph/	Block	14

10-22-2015-20:04:06 to 10-22-2015-21:04:06