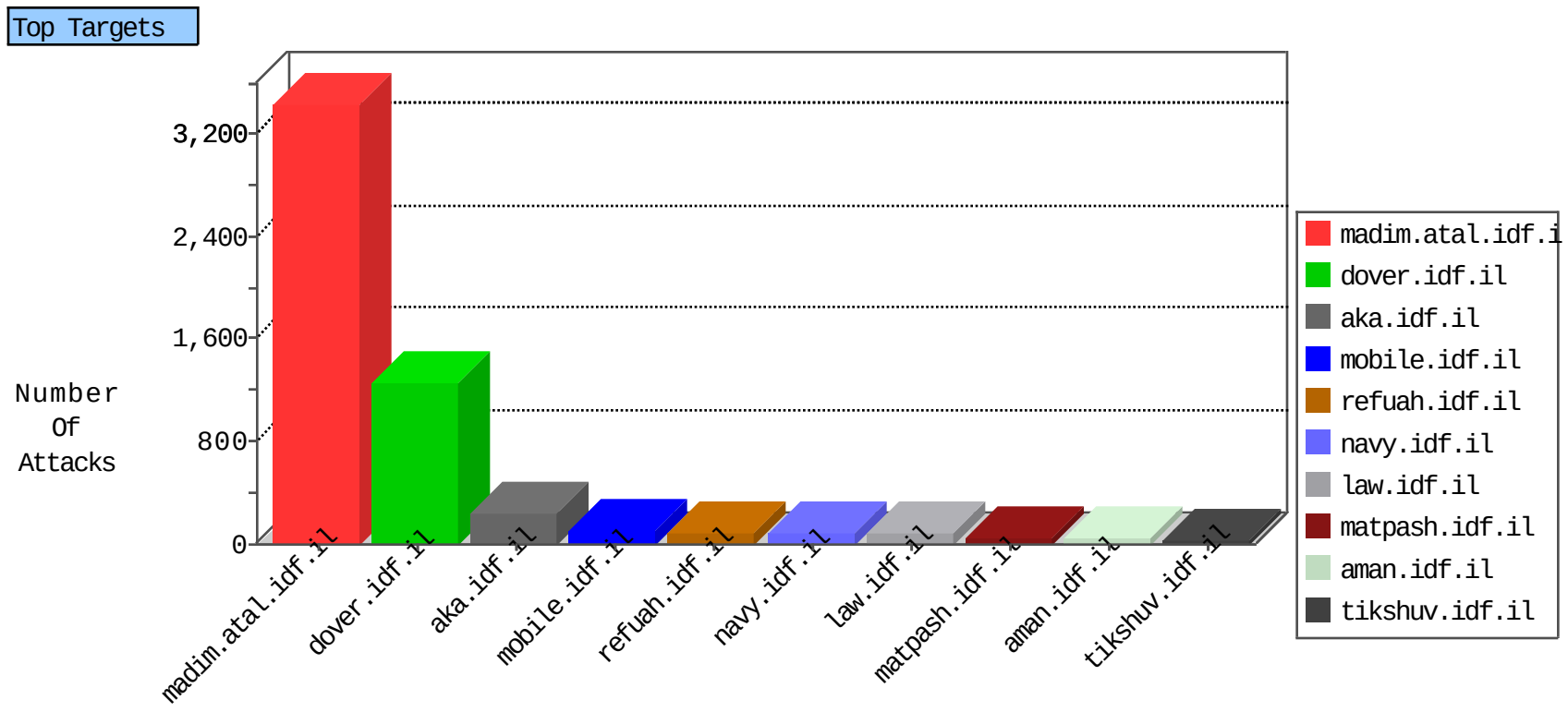
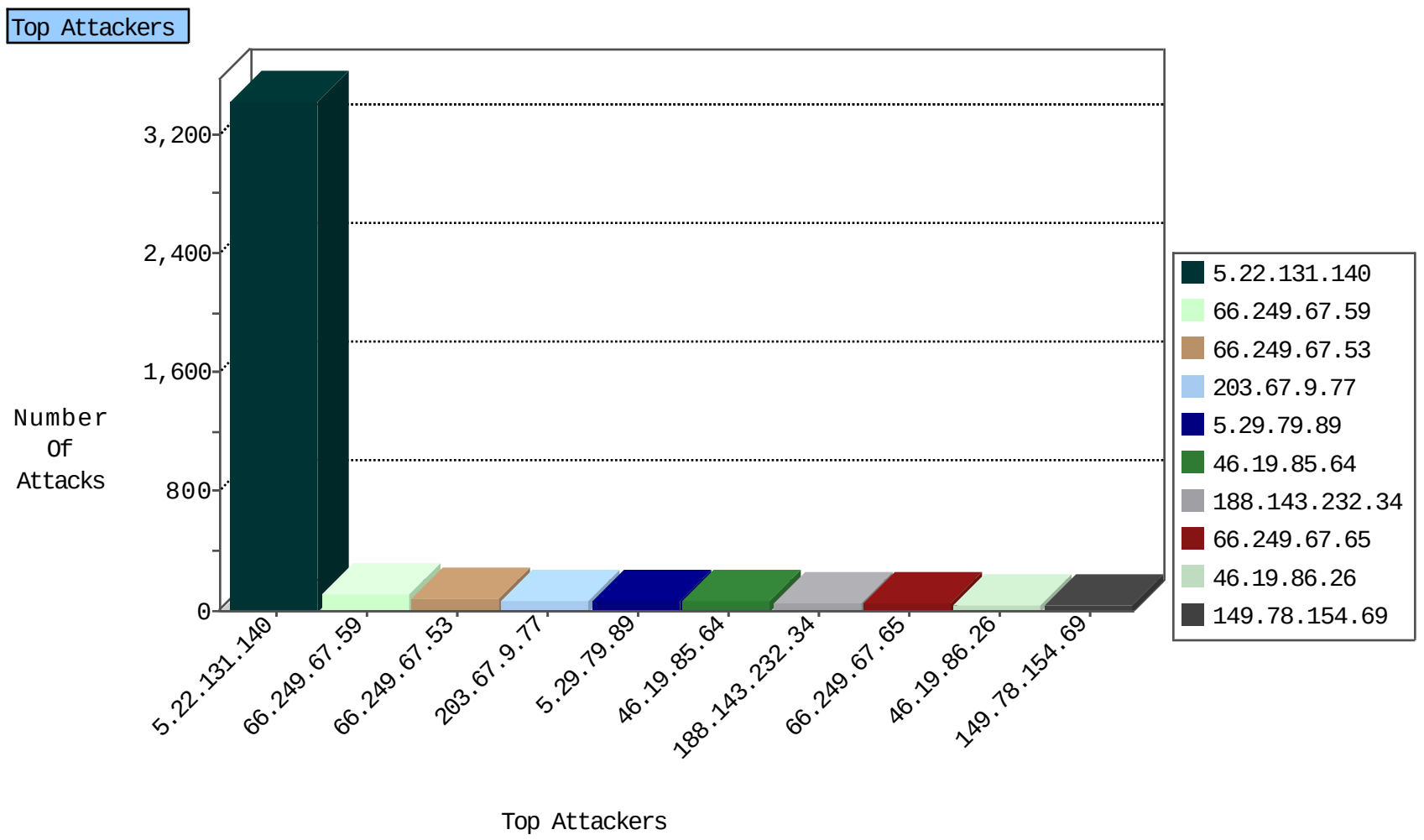
10-25-2015-06:04:04 to 10-25-2015-07:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-06:04:04 to 10-25-2015-07:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.129.15	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	25
69.119.117.117	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
79.143.182.232	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

10-25-2015-06:04:04 to 10-25-2015-07:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-25-2015-06:04:04 to 10-25-2015-07:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.12.145.255	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
176.12.145.255	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
93.174.93.138	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.52.8	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
188.68.224.151	147.237.0.15	Poland	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
188.68.224.151	147.237.0.15	Poland	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
182.48.105.216	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.214.219	147.237.76.148	Singapore	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.194	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.138	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.138	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.74	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
188.68.224.151	147.237.0.15	Poland	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.192.211.88	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.199.214.219	147.237.76.176	Singapore	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.199.214.219	147.237.76.34	Singapore	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.138	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-25-2015-06:04:04 to 10-25-2015-07:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
46.19.86.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
109.64.109.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	24
176.13.5.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
5.29.170.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.40.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.198.86.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.0.80.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.160.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.67.140.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.62.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.132.48.223	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.128.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.241.229.237	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.168.170.190	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.241.237.240	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
100.2.198.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
99.237.184.189	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.225.188	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.46.36.170	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
85.250.120.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
1.128.96.136	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.149.243	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.221.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.165.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.18.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

10-25-2015-06:04:04 to 10-25-2015-07:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.131.140	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.131.140	Block	3423
46.19.85.64	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	70
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	42
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	42
188.143.232.34	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$ddlSearchPlaces in www.law.idf.il/656-he/patzar.aspx	Block	42
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	42
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	28
176.12.143.82	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	28
108.174.155.68	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	14
203.67.9.77	Taiwan	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
74.63.254.220	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	14
188.143.232.35	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/656-en/	Block	14
176.106.227.222	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
79.180.231.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
66.249.67.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1158-he/dover.aspx	Block	14
203.67.9.77	Taiwan	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 203.67.9.77 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	14
66.249.64.253	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1880	Block	14
109.65.211.30	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
203.133.169.32	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
74.82.47.4	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	14
196.22.132.25	South Africa	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	14
182.118.70.144	China	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/../shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	14
79.182.98.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-18008-en/dover.aspx	Block	14
203.67.9.77	Taiwan	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 203.67.9.77 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	14
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/900-en/	Block	14
66.249.65.48	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/faq.aspx	Block	14
157.55.39.38	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/iturim/asp/results.asp	None	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unknown Parameter 387bf100 in aka.idf.il/iturim/asp/results.asp	None	14
79.170.40.38	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/3/size220x0/15863.jpg	Block	14
184.168.27.42	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	14
84.228.34.170	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/general/default.asp	None	14
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
203.67.9.77	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
157.55.39.38	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/results.asp	None	14
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	14
79.178.221.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	14
199.16.156.125	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.125	Block	14
185.32.179.83	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 185.32.179.83 (Open Mode)	None	14
89.138.78.160	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
203.67.9.77	Taiwan	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
188.143.232.34	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$ddlSearchPlaces in www.mag.idf.il/656-he/patzar.aspx	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	14
79.180.231.237	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	14
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17418.jpg	Block	14

10-25-2015-06:04:04 to 10-25-2015-07:04:04