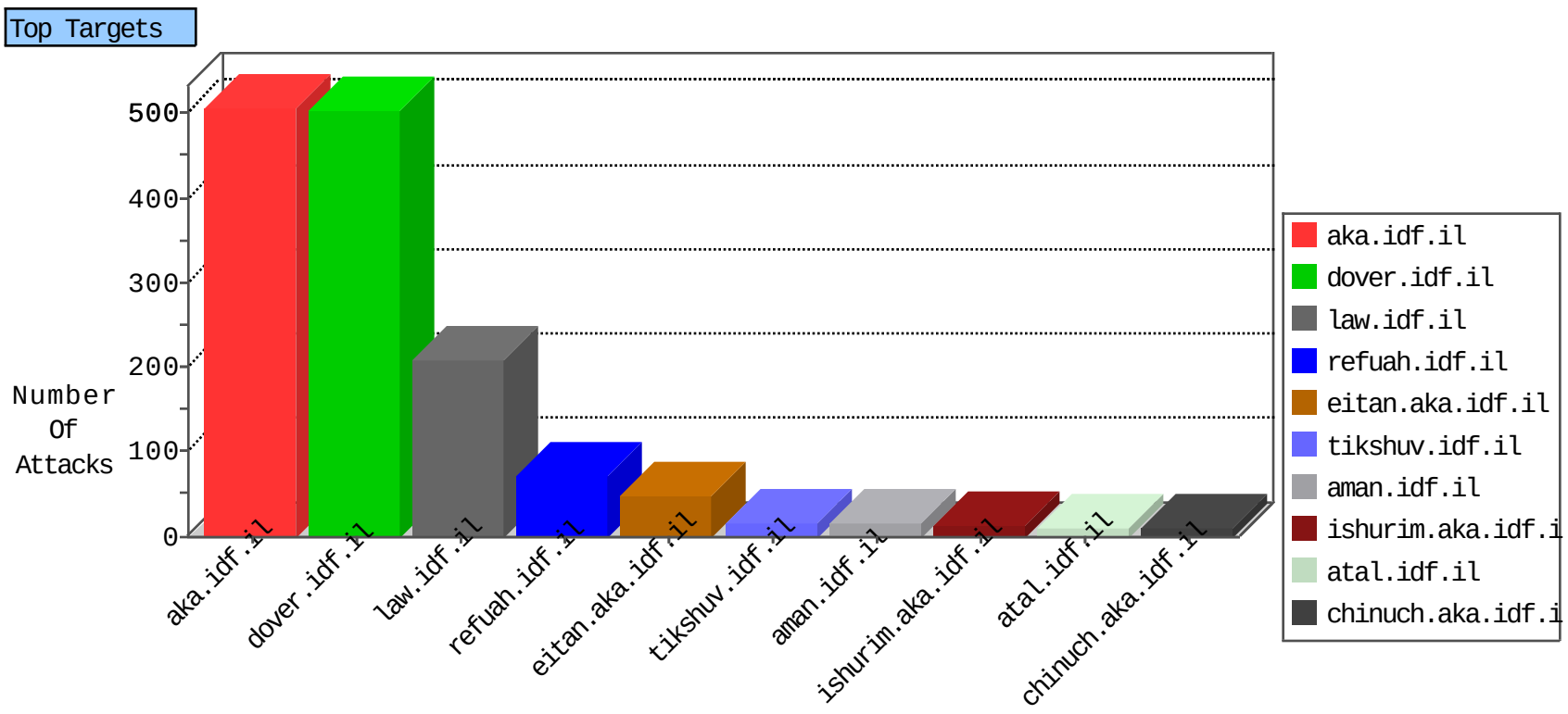
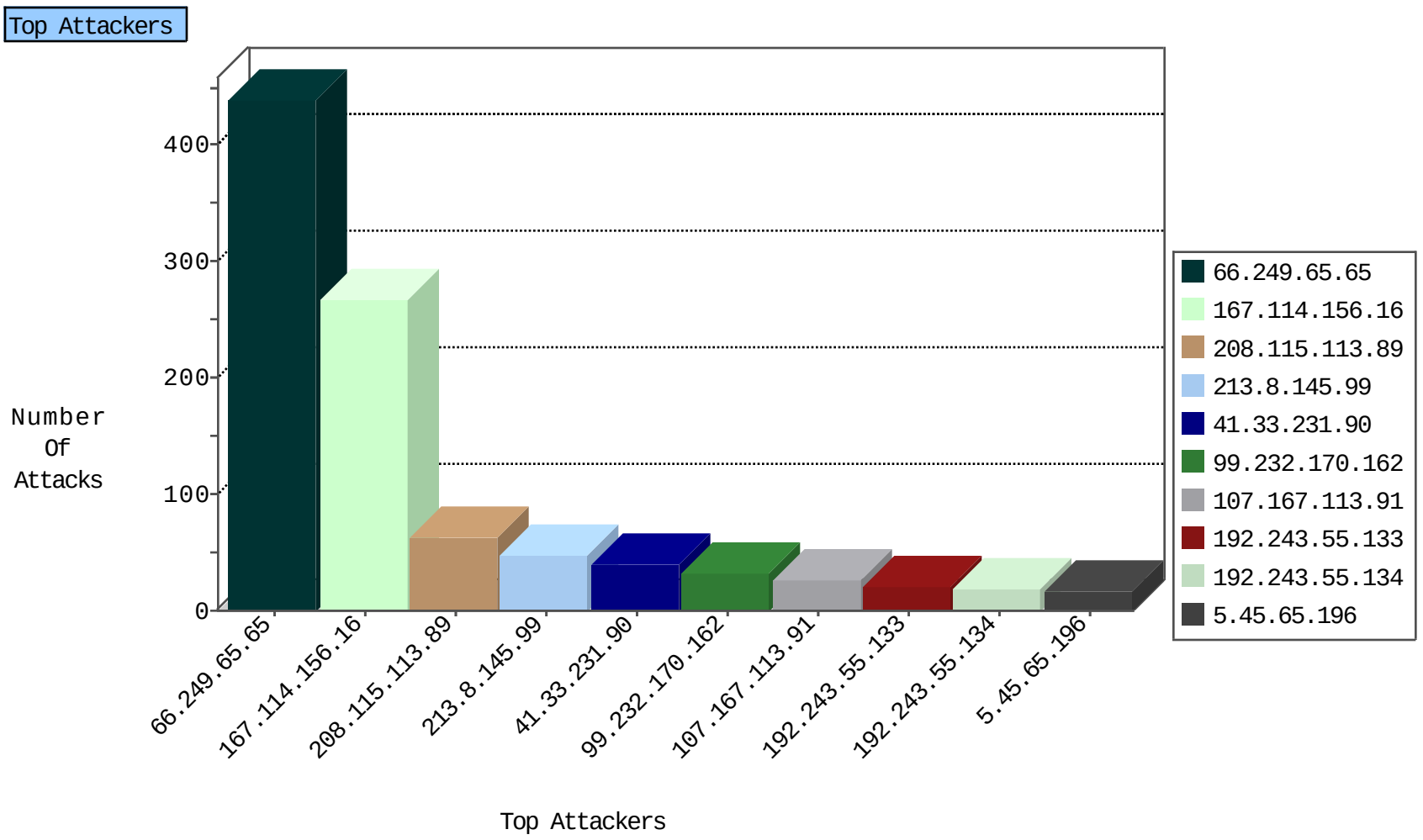
04-22-2016-01:05:32 to 04-22-2016-02:05:32

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-22-2016-01:05:32 to 04-22-2016-02:05:32

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	HTTP-POST-Segmented-DoS	dest-reset	12317
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	324
76.178.133.63	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	215
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
66.249.65.65	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

04-22-2016-01:05:32 to 04-22-2016-02:05:32

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.145.99	Israel	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
177.185.194.47	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.121	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
37.205.0.49	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.45.65.196	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
64.31.44.6	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
5.45.65.196	Netherlands	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
213.8.145.99	Israel	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
95.211.70.193	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.77	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.194.92	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
94.245.88.250	United Kingdom	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
177.185.194.92	Brazil	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
94.245.88.135	United Kingdom	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
66.96.128.60	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
213.8.145.99	Israel	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
94.245.88.250	United Kingdom	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
94.245.88.135	United Kingdom	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

04-22-2016-01:05:32 to 04-22-2016-02:05:32

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.8.145.99	147.237.76.42	Israel	refuah.idf.il	SQL Injection - Select From	36
23.91.70.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	10
94.245.88.250	147.237.76.42	United Kingdom	refuah.idf.il	SQL Injection - Select From	10
23.91.70.121	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
177.185.194.92	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	9
66.96.128.60	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
37.205.0.49	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
177.185.194.47	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
95.211.70.193	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	6
5.45.65.196	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	5
94.245.88.135	147.237.76.42	United Kingdom	refuah.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
221.6.32.82	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
93.174.164.49	147.237.76.177	Romania	ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.226.31.210	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.65.65	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1
221.6.32.82	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
220.231.195.122	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.178.142	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.99	147.237.76.201	Lithuania	e.atal.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
221.226.31.210	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -f -sS	1

04-22-2016-01:05:32 to 04-22-2016-02:05:32

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	417
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
99.232.170.162	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
107.167.113.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
93.172.234.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.105.42.16	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
203.133.170.155	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
95.86.104.64	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
94.73.150.148	Turkey	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.73.243	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.241	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.255.212.83	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.0.112.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
5.45.65.196	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
93.89.19.29	Turkey	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
85.130.231.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.236.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.86.7	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.220.82	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.180.236.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

04-22-2016-01:05:32 to 04-22-2016-02:05:32

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.65	Block	16
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	11
37.26.149.135	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.121.107.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	3
17.138.55.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/iaf.org.il	Block	2
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
81.218.202.150	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 81.218.202.150	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/kamlar/klali/default.asp	None	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9703-he/refuah.aspx	Block	1
54.86.145.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
192.243.55.133	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhllyta1ltawmy5kb2m=&infocenteritem=true	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter list in www.aka.idf.il/megurim/news/	None	1
5.22.134.193	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.50.124.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gen204	Block	1
69.9.106.159	Canada	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
54.190.66.249	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
198.58.103.92	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
93.172.234.72	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
149.78.237.101	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
79.177.232.146	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 79.177.232.146	Block	1
199.30.16.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.173.248.28	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.84	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.177.232.146	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/mobile	Block	1
207.46.13.126	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/main/giyus/giyus/general.aspx	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm	Block	1

04-22-2016-01:05:32 to 04-22-2016-02:05:32