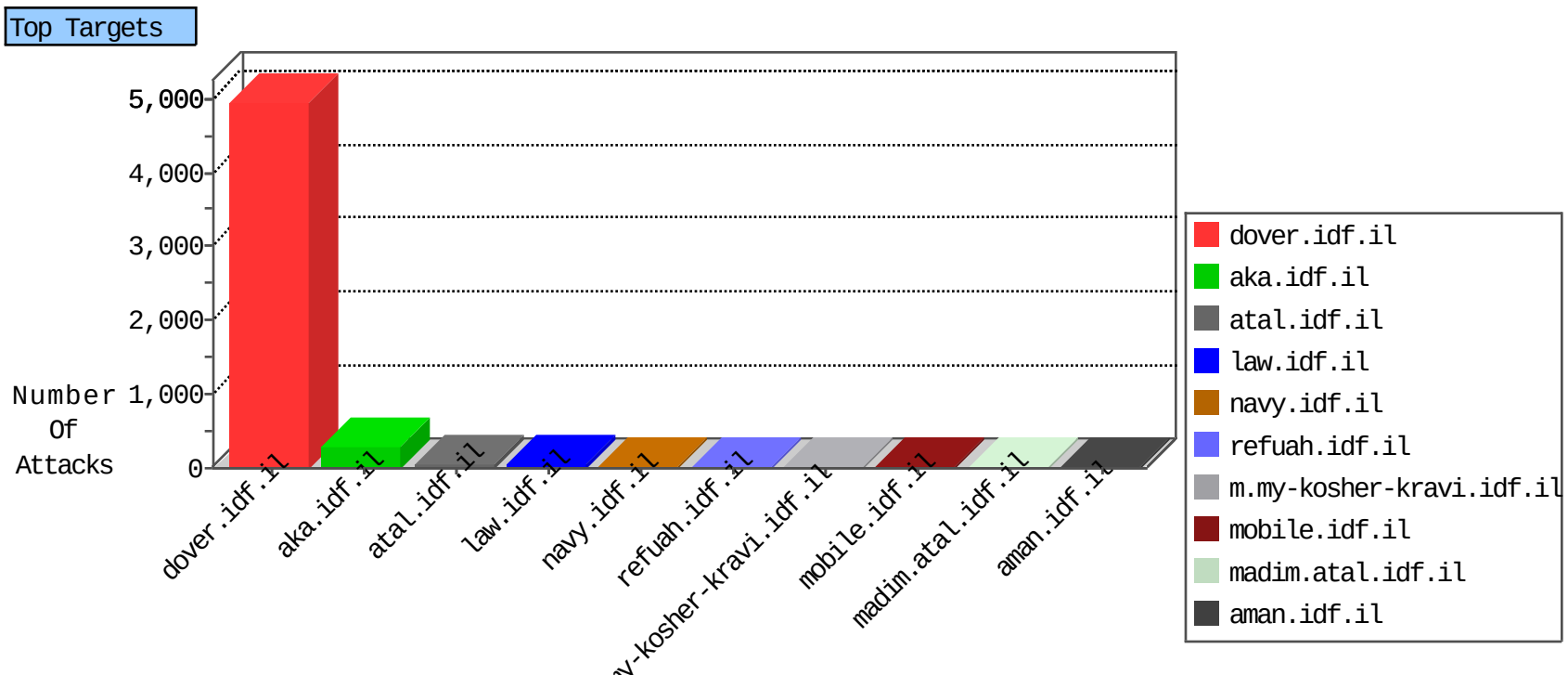
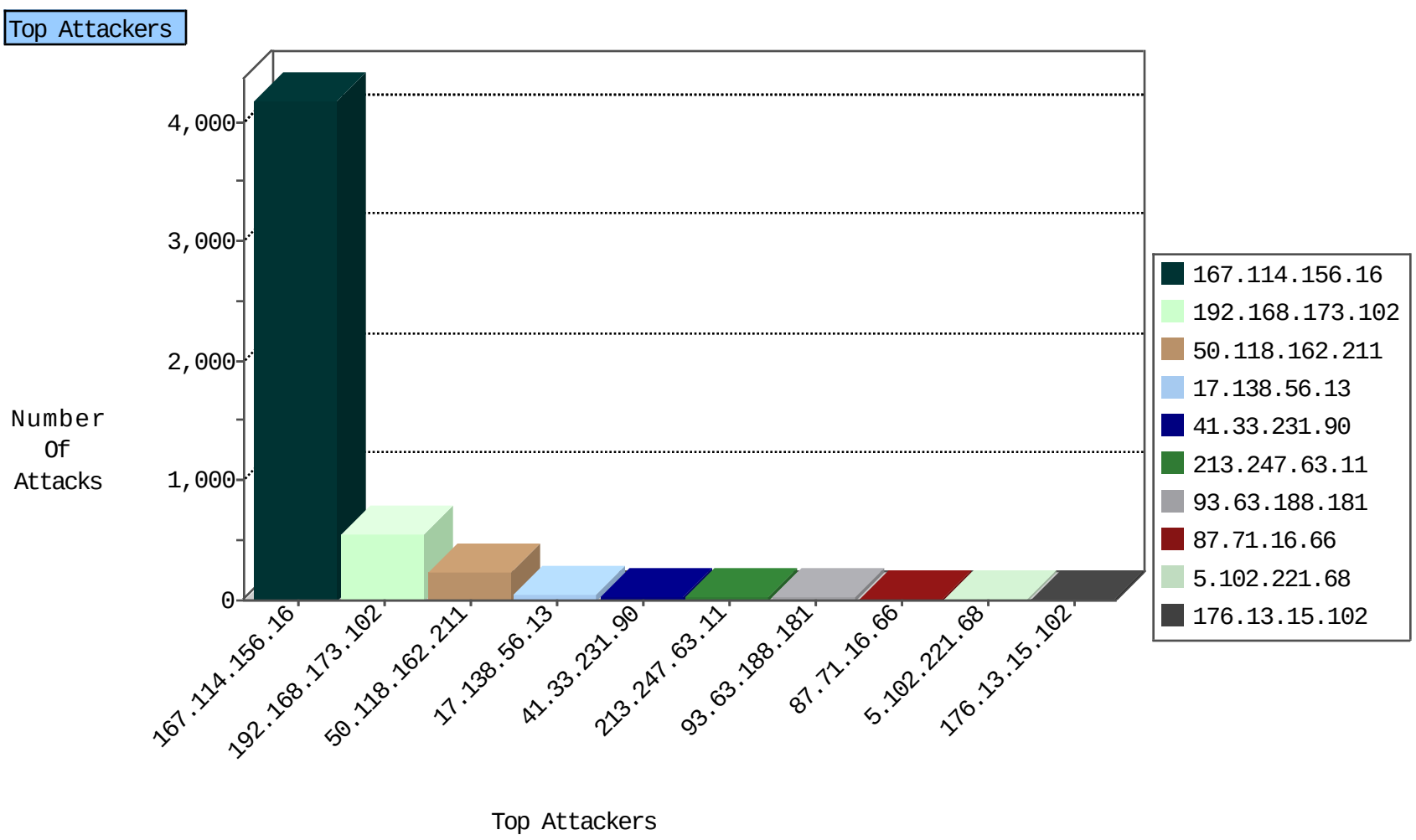
04-09-2016-09:04:00 to 04-09-2016-10:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-09-2016-09:04:00 to 04-09-2016-10:04:00

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	Block_Ip_Web_In	drop	4173
50.118.162.211	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	311
120.132.50.135	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.122	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.78	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.114	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.126	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
31.168.193.248	Israel	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.118	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.126	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
61.183.150.173	China	147.237.0.35	akaws.idf.il	Invalid TCP Flags	drop	1

04-09-2016-09:04:00 to 04-09-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.63.188.181	Italy	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
93.63.188.181	Italy	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.247.63.11	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.247.63.11	Netherlands	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
82.165.24.123	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
162.210.196.129	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.62	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
78.170.35.135	Turkey	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-09-2016-09:04:00 to 04-09-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.247.63.11	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	24
93.63.188.181	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	12
82.165.24.123	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	6
37.187.34.14	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
84.111.152.251	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
42.113.132.39	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -sS window 2048	1
14.29.84.252	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Tomcat Web Application Manager scanning	1
122.173.219.227	147.237.0.35	India	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.76.196	Canada	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
42.113.132.39	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -sS window 4096	1
42.113.132.39	147.237.76.30	Vietnam	himush.idf.il	ET SCAN NMAP -f -sS	1
212.83.181.47	147.237.77.176	France	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
14.29.84.252	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
115.230.150.99	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.183.201.2	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
89.255.21.58	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
50.60.153.98	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1

04-09-2016-09:04:00 to 04-09-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	368
50.118.162.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	226
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	188
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
87.71.16.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.102.221.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.15.102	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.154.174.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
64.46.23.242	Canada	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.186	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
104.138.224.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
177.242.161.48	Mexico	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
98.19.222.133	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
182.184.79.28	Pakistan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.64.30.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.146.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.162.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.43.132	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.194.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.55.60.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.187.34.14	France	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Linux System Files Information Disclosure	reject	2
105.105.158.90	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.116.56.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.116.56.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.88.113.238	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.116.56.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
157.55.39.194	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.144.38	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.23	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
175.136.170.130	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
50.117.96.84	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.211	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
195.62.53.168	Russian Federation	147.237.0.33	idf.il	drop		drop	1
14.29.84.252	China	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
84.111.28.218	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.118	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.28	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

04-09-2016-09:04:00 to 04-09-2016-10:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.170.35.135	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.170.35.135	Block	4
98.143.112.201	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 98.143.112.201	Block	3
78.170.35.135	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
37.187.34.14	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.187.34.14	Block	3
78.170.35.135	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 78.170.35.135	Block	2
37.187.34.14	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20038-he/dover.aspx<span style='color:red	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Header Name at [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[0]]	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
85.250.20.80	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
213.57.201.92	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.75.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.117.135.60	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in URL [[#20]]´[[#21]]¨Ý5c¸¢y•j+²| Š[[#30]]Ÿ¥Ý'ƒœ¨®j[[#0]][[#0]][[#28]],/,+,0,,,[[#19]],	Block	1
169.229.3.90	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/ts.php	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'/m2	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
199.30.16.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
14.29.84.252	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/manager/html	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.79.6	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 103 cookies	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Illegal HTTP Version À[[#20]]À	Block	1
176.13.15.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	NULL Character in URL [[#20]]´[[#21]]¨Ý5c¸¢y•j+²[[Š|#30Ý¥Ÿ]]'ƒ œ¨®j[[#0]][[#0]][[#28]],/,+,0,,,[[#19]],	Block	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
98.143.112.201	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
68.180.229.215	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	1
65.55.210.122	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Malformed HTTP Header Line 1	Block	1
180.76.15.142	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;sideScroll in www.aka.idf.il/giyus/contact/	None	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
120.132.50.135	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.ctrip.com/1149-he/lifestyle.aspx	Block	1
74.82.47.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.65.224	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/links/links.aspx	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Malformed URL [[#20]]´[[#21]]¨Ý5c¸¢y•j+²[[Š|#30Ý¥Ÿ]]'ƒ œ¨®j[[#0]][[#0]][[#28]],/,+,0,,,[[#19]],	Block	1
185.3.144.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
78.170.35.135	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'/m2 in URL [[#20]]´[[#21]]¨Ý5c¸¢y•j+²[[Š|#30Ý¥Ÿ]]',,0,+,/,]]82#[[]]0#[[]]0#[[j®¨Œœƒ [[#19]],	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
37.187.34.14	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/api/xmlrpc	Block	1
209.114.36.145	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]'/m2	Block	1
169.229.3.90	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/ts.php	Block	1
78.170.35.135	Turkey	147.237.77.216	dover.idf.il	Admin Blocking	Block	1

04-09-2016-09:04:00 to 04-09-2016-10:04:00