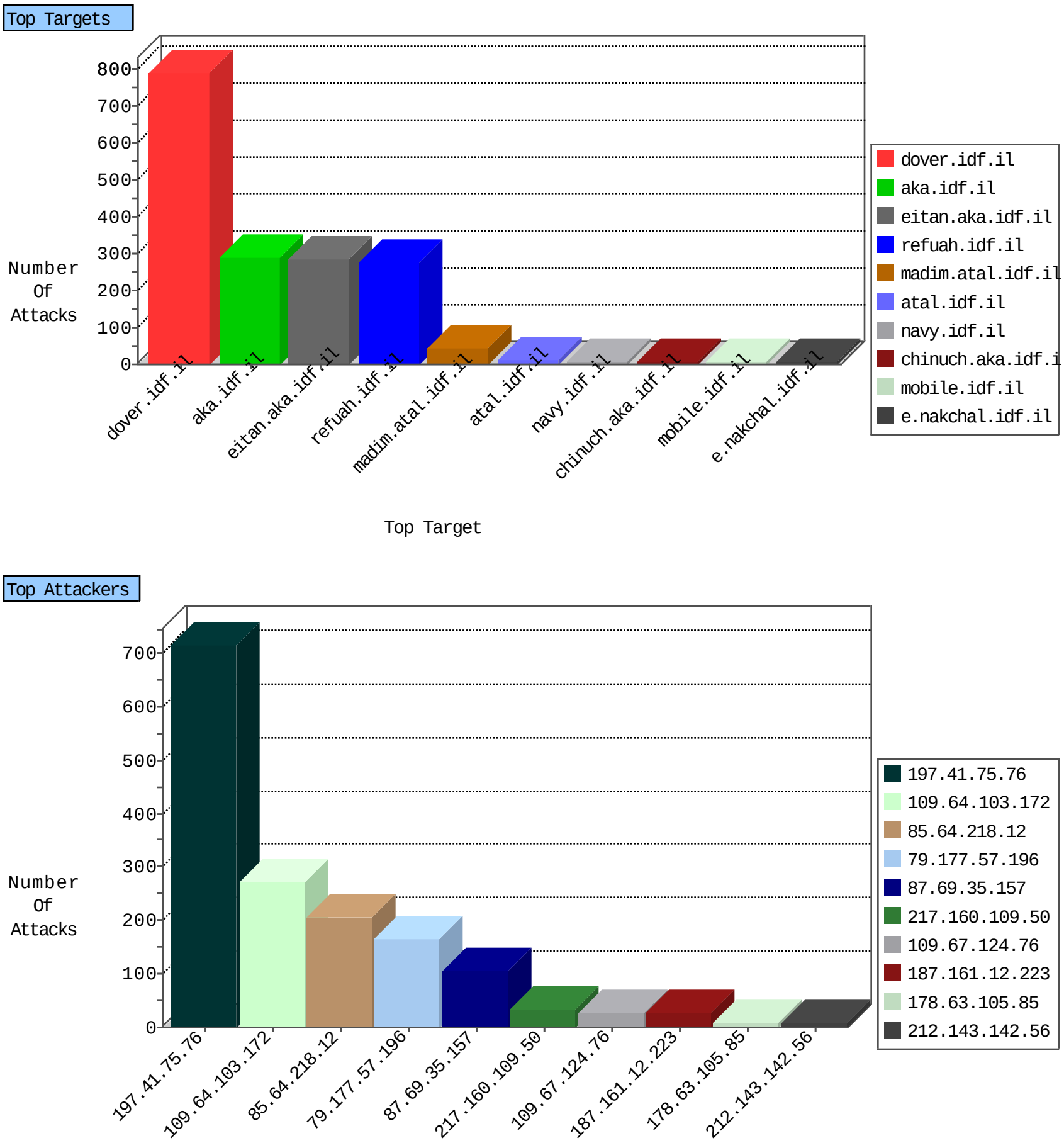
03-05-2016-09:04:08 to 03-05-2016-10:04:08

IDF Under Attack
Daily Report



03-05-2016-09:04:08 to 03-05-2016-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.41.75.76	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	718
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
184.105.139.78	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.90	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.69	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.203	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	1
184.105.139.102	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.118	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1

03-05-2016-09:04:08 to 03-05-2016-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.17.33	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
175.9.139.65	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-05-2016-09:04:08 to 03-05-2016-10:04:08

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
89.248.172.140	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.95.104	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 4096	1
196.47.173.21	147.237.76.176	Cote D'Ivoire	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
196.47.173.21	147.237.76.176	Cote D'Ivoire	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
185.110.132.54	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
159.122.254.235	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.77.27.238	147.237.77.243	India	mobile.idf.il	GPL SCAN nmap TCP	1
95.130.13.220	147.237.77.234	France	halag.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.140	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.69.71	147.237.76.31	France	nakchal.idf.il	ET SCAN Potential SSH Scan	1
200.165.151.203	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.75.95.104	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.176	Cote D'Ivoire	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
159.122.254.235	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
159.122.220.108	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.77.243	France	mobile.idf.il	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.8.50	France	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

03-05-2016-09:04:08 to 03-05-2016-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.103.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	273
85.64.218.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
79.177.57.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	165
87.69.35.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	104
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.185	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.254.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.219.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.163.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.210.186.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
187.161.12.223	Mexico	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
157.55.39.58	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
187.161.12.223	Mexico	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
187.161.12.223	Mexico	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
187.161.12.223	Mexico	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
187.161.12.223	Mexico	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
187.161.12.223	Mexico	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
89.145.95.42	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.115.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
87.71.50.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
187.161.12.223	Mexico	147.237.76.148	gqcenter.aka.idf.il	drop		drop	2
80.246.136.96	Israel	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
69.30.214.46	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
5.22.131.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.67	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.108.240.75	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	2
5.22.135.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.242.198	Canada	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
207.46.13.111	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.135.118	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.127.222.68	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.202.98.161	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
5.29.250.66	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
89.138.170.192	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
2.54.163.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
109.253.204.64	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.71	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.219.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
93.174.95.64	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.248.227.164	Slovakia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
65.19.167.130	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1

03-05-2016-09:04:08 to 03-05-2016-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.124.76	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	28
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	4
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 217.160.109.50	Block	3
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 217.160.109.50	Block	3
46.119.127.64	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 217.160.109.50	Block	3
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 217.160.109.50	Block	3
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 217.160.109.50	Block	3
46.19.86.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Malformed URL from 217.160.109.50	Block	3
82.81.98.120	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.81.98.120	Block	3
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 217.160.109.50	Block	3
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 217.160.109.50	Block	3
109.205.248.38	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/forum/asp/showforum.asp	Block	2
46.119.122.177	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	2
82.81.98.120	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
217.160.109.50	Germany	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.58	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
89.139.176.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main	Block	1
79.178.223.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Too Many Headers per Request from 217.160.109.50	Block	1
40.77.167.14	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
117.81.227.193	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
82.154.230.129	Portugal	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.58	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/news/news.in.aspx	Block	1
89.139.176.222	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
81.1.196.254	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
40.77.167.92	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Illegal HTTP Version •À 9ÛßÆ([[#7]]…Ž8 ,ƒÉá—dm÷‰å[[#25]]a‹ßC[[#3]]^[[#2]]$ŒåÅk[[#28]]&'"“üÕ 7Ù[[#17]][[#14]][[#20]]›¾åè«[[#23]]Ämé½Ì×kó¯#012YuT•`•Ùùz6“6ïo[[#31]]*€€;P[[#23]]¦Ú"[[#7]];¥,*ƒKz¬=Â[[#19]].áÑnHùaæX™ùËo`x,ør[[#0]]ŠÉŒ‘ µÜðžì[[#6]][[#11]]í VØ[[#17]]ôUI}üÃ†[[#28]]Z[[#31]]µ[[#3]]^gWÞªq~[[#22]]®žœ¯ŠV~y¢')à˜-ðø,ÂÐ[[#0]][[#8]]•pÂó#011ì¡ä¶[[#8]]ZüÜ¡‰5®2:´Ã´‘¦–š—••*ì[[#23]][[#22]][[#7]]ùV¹Úè—';”à[[#19]]¸kK…[[#30]]ç°“’g¸€[[#25]]k[[#11]]l(~%”•X/Ðç[[#15]]Z`Å-W[[#19]]¯g¨ndõù,±^§ÈÊ±¡è™À3„fÈ—ö—[[#14]]ŸÌx#PVÀÓ»¢tÈpP	Block	1
134.249.131.0	Ukraine	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter f	Block	1
83.17.9.50	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1402-he/atal.aspx	Block	1
187.161.12.223	Mexico	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to /tmunblock.cgi	Block	1
109.64.103.172	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
81.1.196.254	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
217.160.109.50	Germany	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.160.109.50 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
134.249.131.0	Ukraine	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter l	Block	1
87.69.35.157	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter r in www.eitan.aka.idf.il/templates/opcontactus/govcaptchaimage.axd	None	1
68.180.228.95	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/994-he/nakhal.aspx	Block	1
24.114.69.82	Canada	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
217.160.109.50	Germany	147.237.72.166	aka.idf.il	NULL Character in Method ûÕ[[#15]]œ[>í[[#29]]±Y^/b[[#23]][[#5]]õ<d@ð5?Sñ:Ì&V^™[[#22]]êÍ›šW›•ª ƒó[[#14]]Ï@~•ij/Rëvó†sõ‰Ù˜[[#22]]•ÀõÃþ[[#14]]—¨žé«“ý-•[[#0]][[#20]]× üxÁD[[#30]]ÃÐd¦51[[#17]]z[[#25]][[#0]][[#24]]ú“:	Block	1
149.202.98.161	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
87.71.65.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
74.82.47.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.26.146.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.218.206.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1

03-05-2016-09:04:08 to 03-05-2016-10:04:08