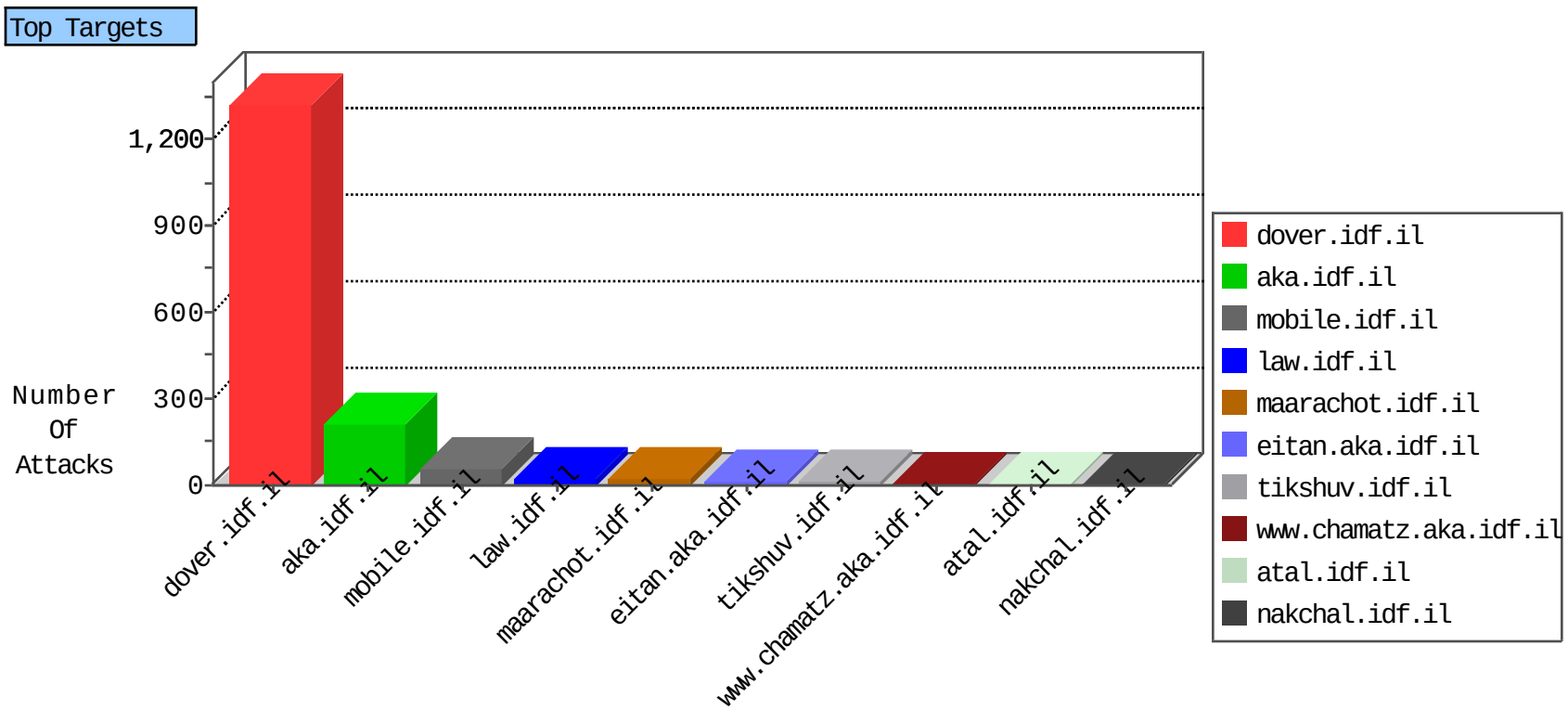
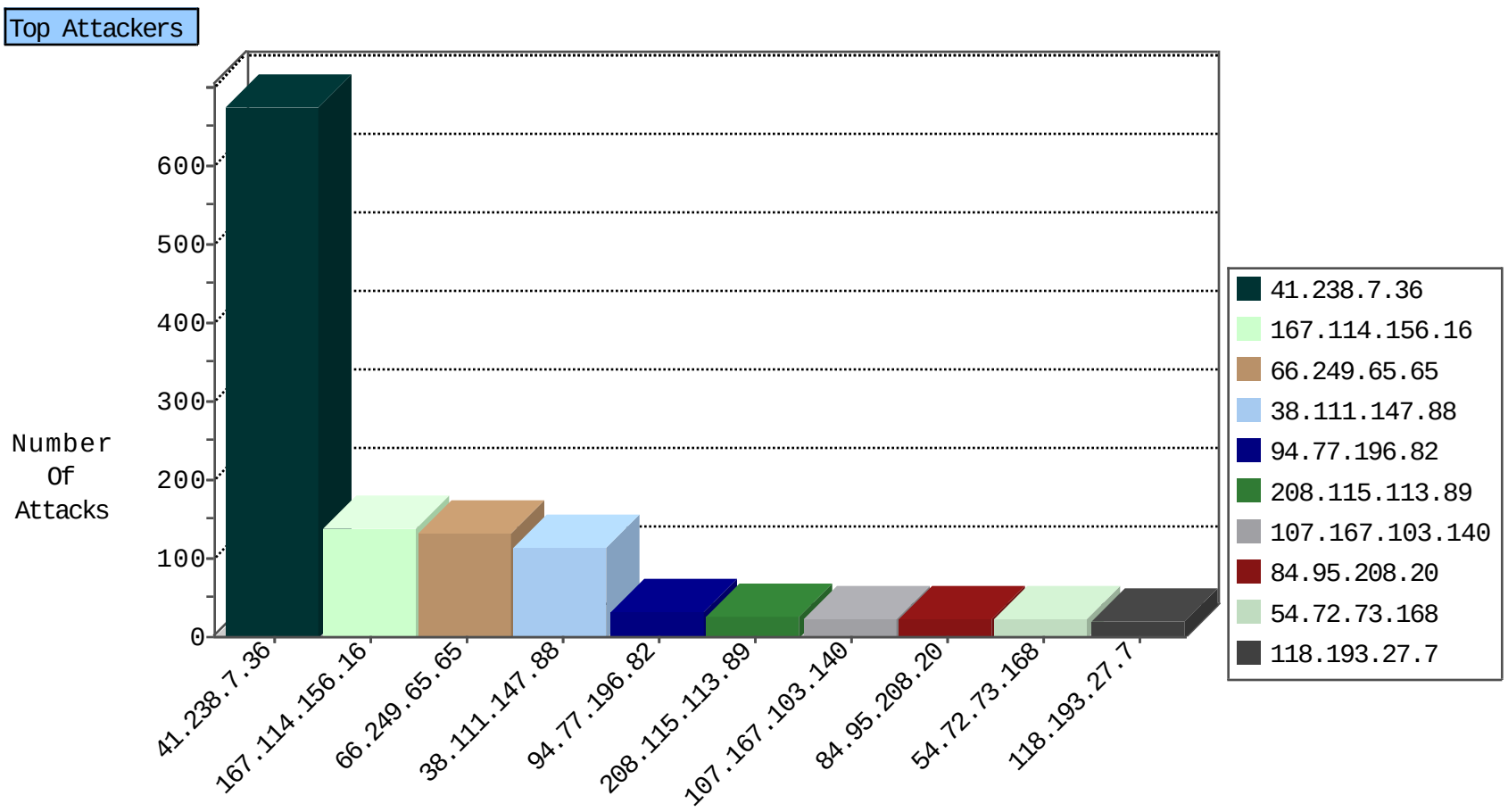
05-04-2016-01:07:24 to 05-04-2016-02:07:24

IDF Under Attack
Daily Report





05-04-2016-01:07:24 to 05-04-2016-02:07:24

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	6471
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
123.151.42.61	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

05-04-2016-01:07:24 to 05-04-2016-02:07:24

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.143.180.166	United States	147.237.77.234	halag.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
41.238.7.36	Egypt	147.237.77.216	dover.idf.i	0863: HTTP: fpadmcgi.exe Access	Block	1
41.238.7.36	Egypt	147.237.77.216	dover.idf.i	1185: HTTP: IIS admcgi CGI Access	Block	1

05-04-2016-01:07:24 to 05-04-2016-02:07:24

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	327
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.79.89	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
84.109.178.243	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.65	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
95.173.184.12	147.237.72.166	Turkey	aka.idf.il	ET SCAN Potential SSH Scan	1
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP server-status access	1
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP active.log access	1
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP .bash_history access	1
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP .DS_Store access	1
202.29.94.108	147.237.76.198	Thailand	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
118.193.27.7	147.237.77.170	Hong Kong	maarachot.idf.il	ET WEB_SERVER Poison Null Byte	1
91.197.232.40	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP server-info access	1
41.238.7.36	147.237.77.216	Egypt	dover.idf.il	SERVER-WEBAPP .FBCIndex access	1
202.170.80.40	147.237.77.235	Mongolia	sviva.idf.il	ET SCAN Potential SSH Scan	1

05-04-2016-01:07:24 to 05-04-2016-02:07:24

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	129
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
41.238.7.36	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
107.167.103.140	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.108.238.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.1.156.207	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.109.18.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.151.209.156	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.178.232.234	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.65.28.146	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.28.146	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.108.238.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
31.168.67.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
165.230.224.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
129.81.78.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
144.76.71.83	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.27.105.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
78.164.126.12	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
8.37.227.69	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.136	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
156.211.138.17	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.241.231.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.238.7.36	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.238.7.36	Block	272
41.238.7.36	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	12
41.238.7.36	Egypt	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.238.7.36	Block	5
5.29.126.145	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	3
84.109.18.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.149.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.116.115.174	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
31.168.67.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Illegal HTTP Version	Block	1
109.66.10.219	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/links/mobile	Block	1
80.86.94.7	Germany	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	1
151.80.31.183	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Illegal HTTP Version from 118.193.27.7	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#1]]"[[#1]][[#0]][[#1]][[#30]][[#3]][[#3]] Ý"E£´[[#6]][[#22]]£[[#27]]‡;T¡ˆ[[#0]]µÈ.¤ÌIë5™{Üöi	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2974.jpg	Block	1
37.26.146.170	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Malformed HTTP Header Line 1	Block	1
109.175.109.33	Bosnia and Herzegovina	147.237.77.74	law.idf.il	PHP Attempt	Block	1
80.86.94.7	Germany	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
185.27.105.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Malformed HTTP Header Line from 118.193.27.7	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Header Name À/À+À'À#À[[#19]]À#011[[#0]]¢[[#0]]ž[[#0]]g[[#0]]@[[#0]]3[[#0]]2[[#0]]š[[#0]]™[[#0]]E[[#0]]DÀ1À-À)À%À[[#14]]À[[#4]][[#0]]œ[[#0]]<[[#0]]/[[#0]]–[[#0]]AÀ[[#17]]À[[#7]]À[[#12]]À[[#2]][[#0]][[#5]][[#0]][[#4]][[#0]][[#21]][[#0]][[#18]][[#0]]#011[[#0]]ÿ[[#1]][[#0]][[#0]]m[[#0]][[#11]][[#0]][[#4]][[#3]][[#0]][[#1]][[#2]][[#0]]	Block	1
85.65.51.168	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	NULL Character in URL [[#25]]‹[[#0]][[#0]]ˆ¸0¸,¸(¸$¸[[#20]]¸	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Malformed URL [[#25]]‹[[#0]][[#0]]ˆ¸0¸,¸(¸$¸[[#20]]¸	Block	1
109.175.109.33	Bosnia and Herzegovina	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Malformed URL from 118.193.27.7	Block	1
41.238.7.36	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/uniscan5513uniscan/	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#1]]"[[#1]][[#0]][[#1]][[#30]][[#3]][[#3]] Ý"E£´[[#6]][[#22]]£[[#27]]‡;T¡ˆ[[#0]]µÈ.¤ÌIë5™{Üöi	Block	1
5.29.126.145	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 5.29.126.145	Block	1
85.65.51.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
41.238.7.36	Egypt	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Abnormally Long Request from 118.193.27.7	Block	1
109.253.208.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Unknown HTTP Request Method from 118.193.27.7	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL [[#25]]‹[[#0]][[#0]]ˆ¸0¸,¸(¸$¸[[#20]]	Block	1
85.65.51.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#1]]"[[#1]][[#0]][[#1]][[#30]][[#3]][[#3]] Ý"E£´[[#6]][[#22]]£[[#27]]‡;T¡ˆ[[#0]]µÈ.¤ÌIë5™{Üöi in URL [[#25]]‹[[#0]][[#0]]ˆ¸0¸,¸(¸$¸[[#20]]¸	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Header Name from 118.193.27.7	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	Abnormally Long Header Line request header name	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/div.item	Block	1
118.193.27.7	Hong Kong	147.237.77.170	maarachot.idf.il	NULL Character in Header Name at [[#0]]£[[#0]]Ÿ[[#0]]k[[#0]]j[[#0]]9[[#0]]8[[#0]]ˆ[[#0]]‡À2À.À*À&À[[#15]]À[[#5]][[#0]]•[[#0]]=[[#0]]5[[#0]]„À[[#18]]À[[#8]][[#0]][[#22]][[#0]][[#19]]À#012À[[#3]][[#0]]	Block	1
65.55.212.68	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1