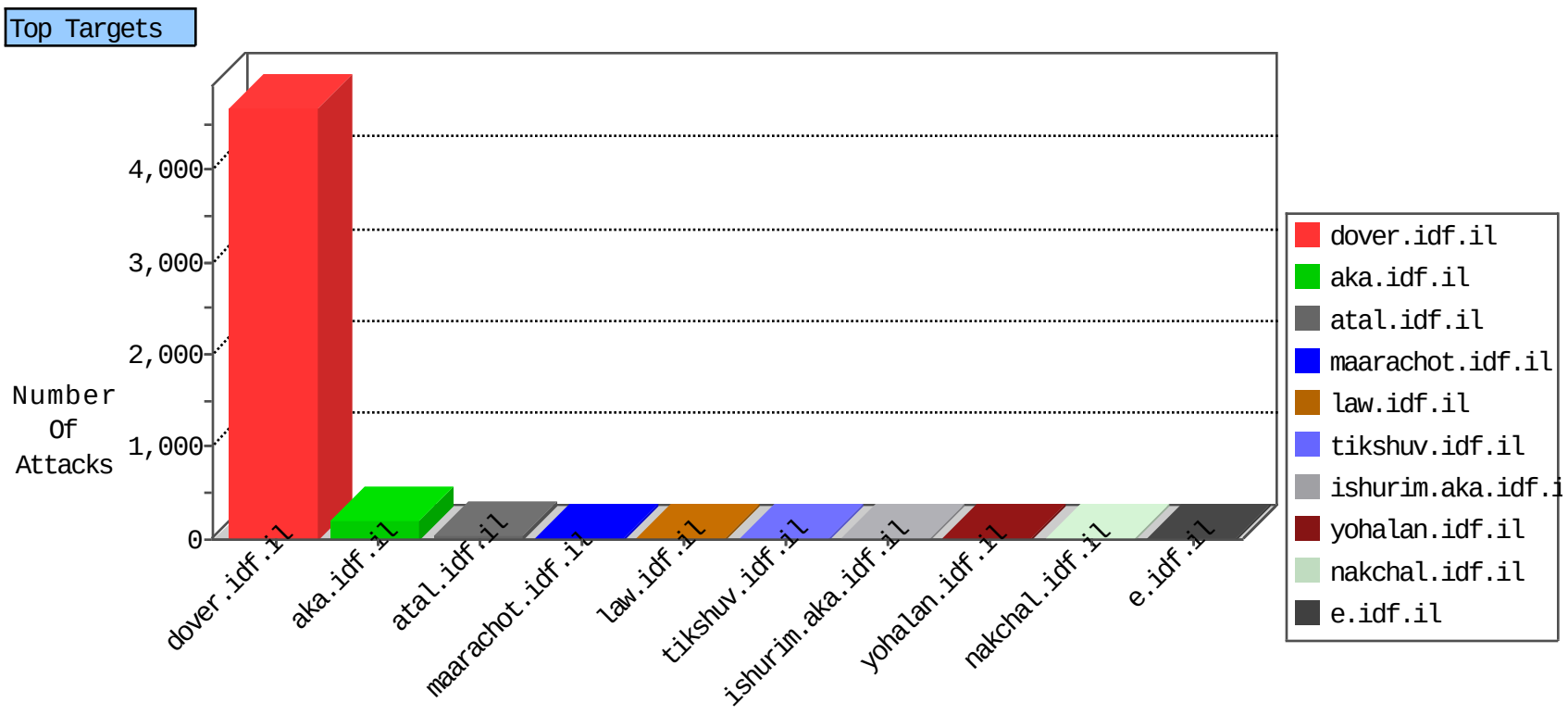
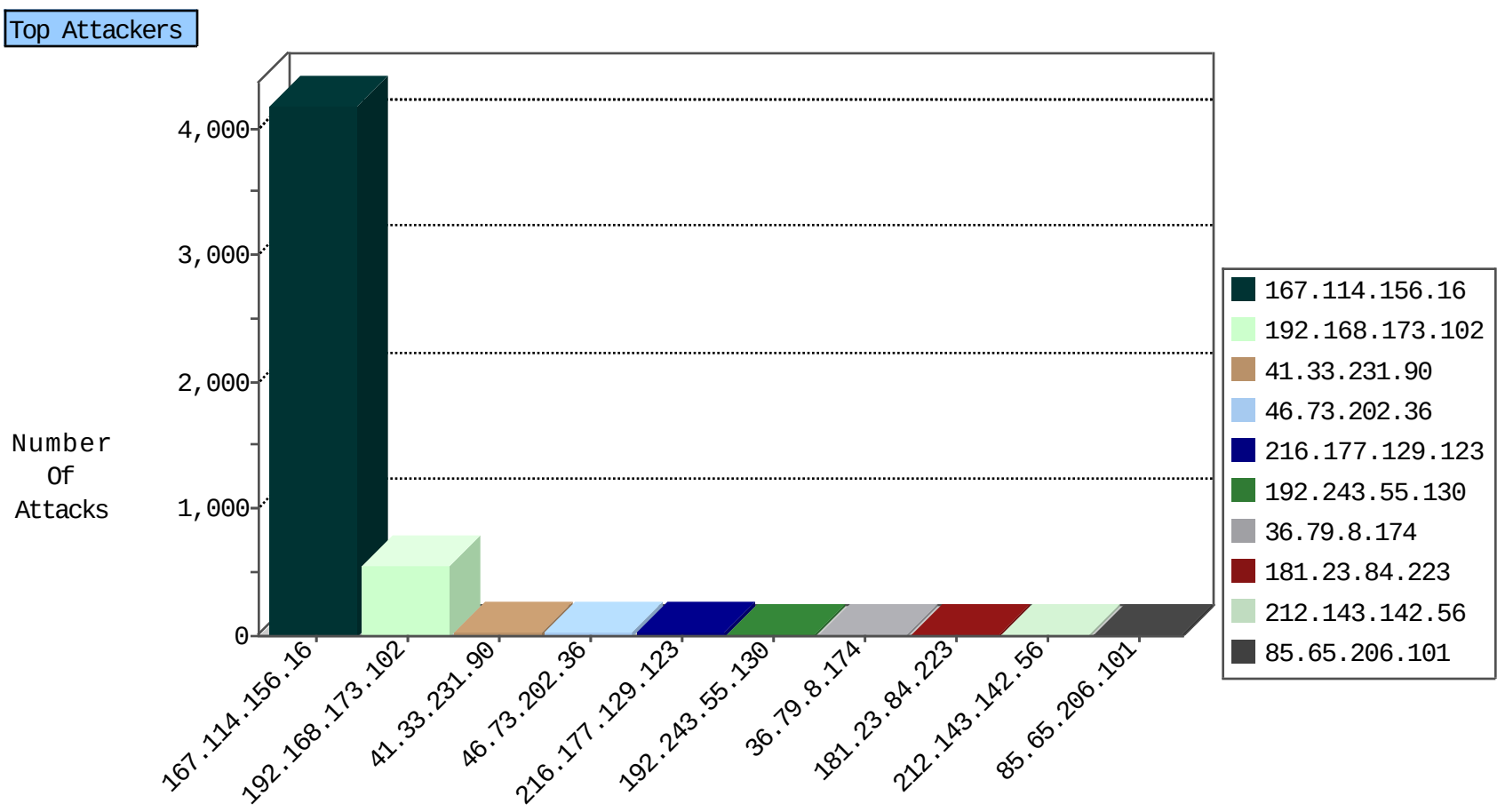
04-11-2016-04:04:08 to 04-11-2016-05:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-11-2016-04:04:08 to 04-11-2016-05:04:08

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	4172
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
219.232.243.28	China	147.237.77.19	law-forum.idf.il	Invalid L4 Header Length	drop	1
123.56.26.146	China	147.237.76.34	yohalan.idf.il	Invalid TCP Flags	drop	1
42.112.10.75	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
179.43.144.50	Switzerland	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.93	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
219.232.243.28	China	147.237.76.30	himush.idf.il	Invalid L4 Header Length	drop	1
115.28.169.142	China	147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	1
38.229.1.13	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.76.201	e.atal.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
219.232.243.28	China	147.237.76.31	nakchal.idf.il	Invalid L4 Header Length	drop	1
121.40.68.51	China	147.237.76.86	navy.idf.il	L4 Source or Dest Port Zero	drop	1
42.112.10.65	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
179.43.144.50	Switzerland	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1

04-11-2016-04:04:08 to 04-11-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.30.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
87.70.59.147	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
87.70.59.147	Israel	147.237.76.86	navy.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
36.79.8.174	Indonesia	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
87.70.59.147	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
36.79.8.174	Indonesia	147.237.77.170	maarachot.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-04:04:08 to 04-11-2016-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
36.79.8.174	147.237.77.74	Indonesia	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
36.79.8.174	147.237.77.170	Indonesia	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
163.172.140.23	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
88.204.187.90	147.237.77.234	Kazakstan	halag.idf.il	ET SCAN NMAP -f -sS	1
188.213.219.175	147.237.72.156	Romania	aman.idf.il	ET SCAN Potential SSH Scan	1
58.218.205.69	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
188.213.219.175	147.237.0.33	Romania	idf.il	ET SCAN Potential SSH Scan	1
185.114.157.12	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.81.18	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.114.157.12	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 2048	1
182.243.102.192	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.140.23	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.1.128.251	147.237.0.33	Tunisia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.204.187.90	147.237.77.234	Kazakstan	halag.idf.il	ET SCAN NMAP -sS window 2048	1
188.213.219.175	147.237.77.19	Romania	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.1.136.6	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.213.219.175	147.237.0.35	Romania	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.114.157.12	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
13.92.81.18	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
185.114.157.12	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
185.114.157.12	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -f -sS	1
175.100.5.158	147.237.0.35	Cambodia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.140.23	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

04-11-2016-04:04:08 to 04-11-2016-05:04:08

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	385
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	167
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.73.202.36	Russian Federation	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
216.177.129.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
181.23.84.223	Argentina	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
149.78.169.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.106.92.47	Russian Federation	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.106.92.47	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
172.58.41.178	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.169.63	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
106.186.113.132	Japan	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.85.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
141.212.122.139	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.56.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.187.114.171	France	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.72	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.128	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.90	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
141.212.122.143	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.98	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
38.229.1.15	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.90	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.129	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.29.199.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.200	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.98	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.130	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.90	United States	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
141.212.122.130	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
200.74.240.180	Panama	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.254.250.121	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	6
181.23.84.223	Argentina	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	5
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
54.153.32.246	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
217.69.133.245	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/reserve	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.194	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	Malformed URL	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
200.74.240.180	Panama	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
141.212.122.129	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /x	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
65.55.210.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam/main/procedure.asp	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	NULL Character in Header Name at [[#0]][[#28]][[#0]][[#26]][[#0]][[#23]][[#0]][[#25]][[#0]][[#28]][[#0]][[#27]][[#0]][[#24]][[#0]][[#26]][[#0]][[#22]][[#0]][[#14]][[#0]]#012[[#0]][[#11]][[#0]][[#12]][[#0]]#011[[#0]]	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.25	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
141.212.122.129	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /x	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Header Name	Block	1
65.55.210.122	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	NULL Character in Method [[#22]][[#3]][[#1]][[#0]]¾[[#1]][[#0]][[#0]]°[[#3]][[#3]]O-¡·œƒ³?Å[[#29]]FÀÔËyf†õ=Òî<Dî5@[[#22]]M±ÙŽ[[#28]][[#0]][[#0]]&À0À(À[[#20]]À/À'À[[#19]][[#0]]Ÿ[[#0]]k[[#0]]9[[#0]]ž[[#0]]g[[#0]]3[[#0]]•[[#0]]=[[#0]]5[[#0]]œ[[#0]]<[[#0]]/[[#0]]ÿ[[#1]][[#0]][[#0]]k[[#0]][[#0]][[#0]][[#23]][[#0]][[#21]][[#0]][[#0]][[#18]]notify.dropbox.com[[#0]][[#11]][[#0]][[#4]][[#3]][[#0]][[#1]][[#2]][[#0]]	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9680-he/refuah.aspx	Block	1
37.187.114.171	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /irj/portal	Block	1
207.46.13.47	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1360-he/atal.aspx	Block	1
141.212.122.129	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /x	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]¾[[#1]][[#0]][[#0]]°[[#3]][[#3]]O-¡·œƒ³?Å[[#29]]FÀÔËyf†õ=Òî<Dî5@[[#22]]M±ÙŽ[[#28]][[#0]][[#0]]&À0À(À[[#20]]À/À'À[[#19]][[#0]]Ÿ[[#0]]k[[#0]]9[[#0]]ž[[#0]]g[[#0]]3[[#0]]•[[#0]]=[[#0]]5[[#0]]œ[[#0]]<[[#0]]/[[#0]]ÿ[[#1]][[#0]][[#0]]k[[#0]][[#0]][[#0]][[#23]][[#0]][[#21]][[#0]][[#0]][[#18]]notify.dropbox.com[[#0]][[#11]][[#0]][[#4]][[#3]][[#0]][[#1]][[#2]][[#0]]	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
194.187.168.194	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]¾[[#1]][[#0]][[#0]]°[[#3]][[#3]]O-¡·œƒ³?Å[[#29]]FÀÔËyf†õ=Òî<Dî5@[[#22]]M±ÙŽ[[#28]][[#0]][[#0]]&À0À(À[[#20]]À/À'À[[#19]][[#0]]Ÿ[[#0]]k[[#0]]9[[#0]]ž[[#0]]g[[#0]]3[[#0]]•[[#0]]=[[#0]]5[[#0]]œ[[#0]]<[[#0]]/[[#0]]ÿ[[#1]][[#0]][[#0]]k[[#0]][[#0]][[#0]][[#23]][[#0]][[#21]][[#0]][[#0]][[#18]]notify.dropbox.com[[#0]][[#11]][[#0]][[#4]][[#3]][[#0]][[#1]][[#2]][[#0]] in URL	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
157.55.2.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.65.206.101	Israel	147.237.77.170	maarachot.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
197.231.221.211	Liberia	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
87.70.59.147	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1