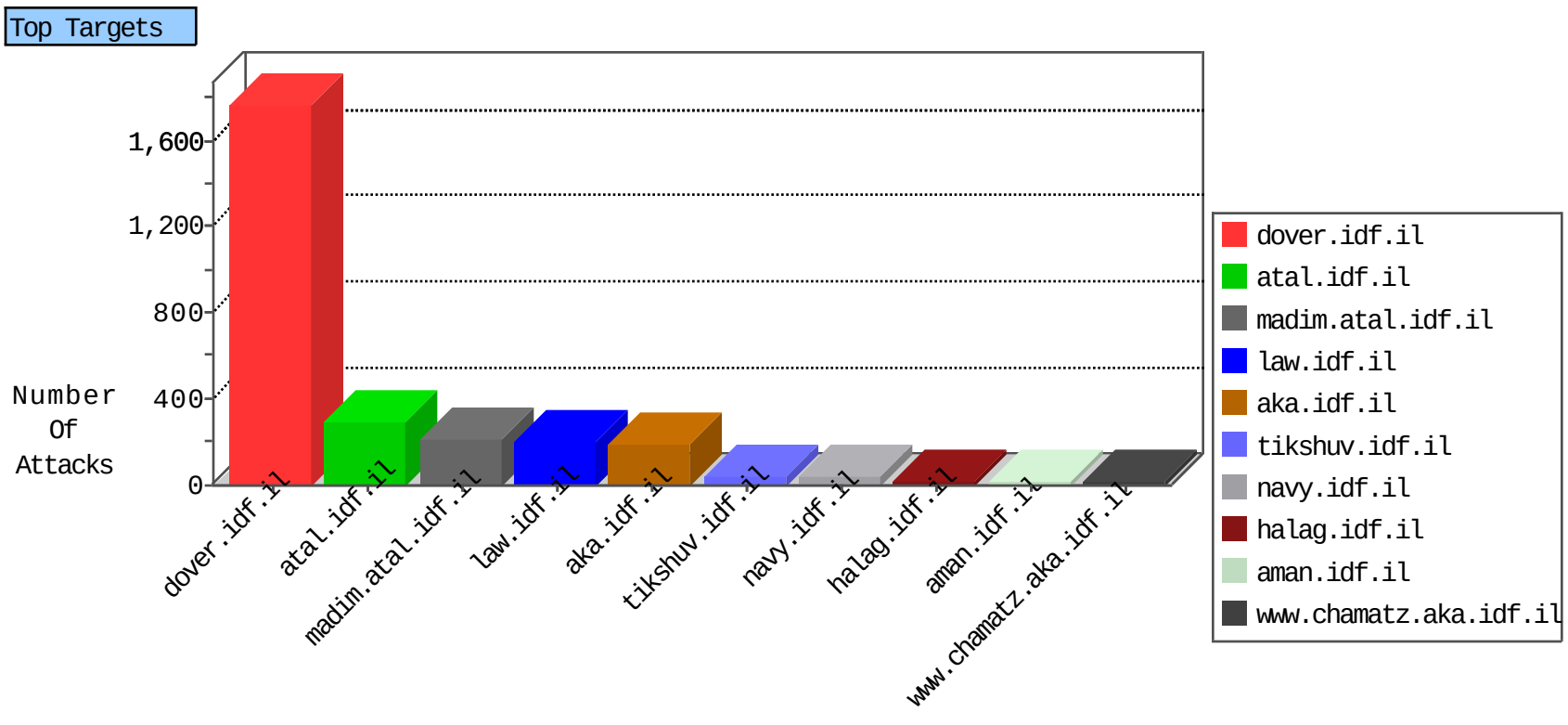
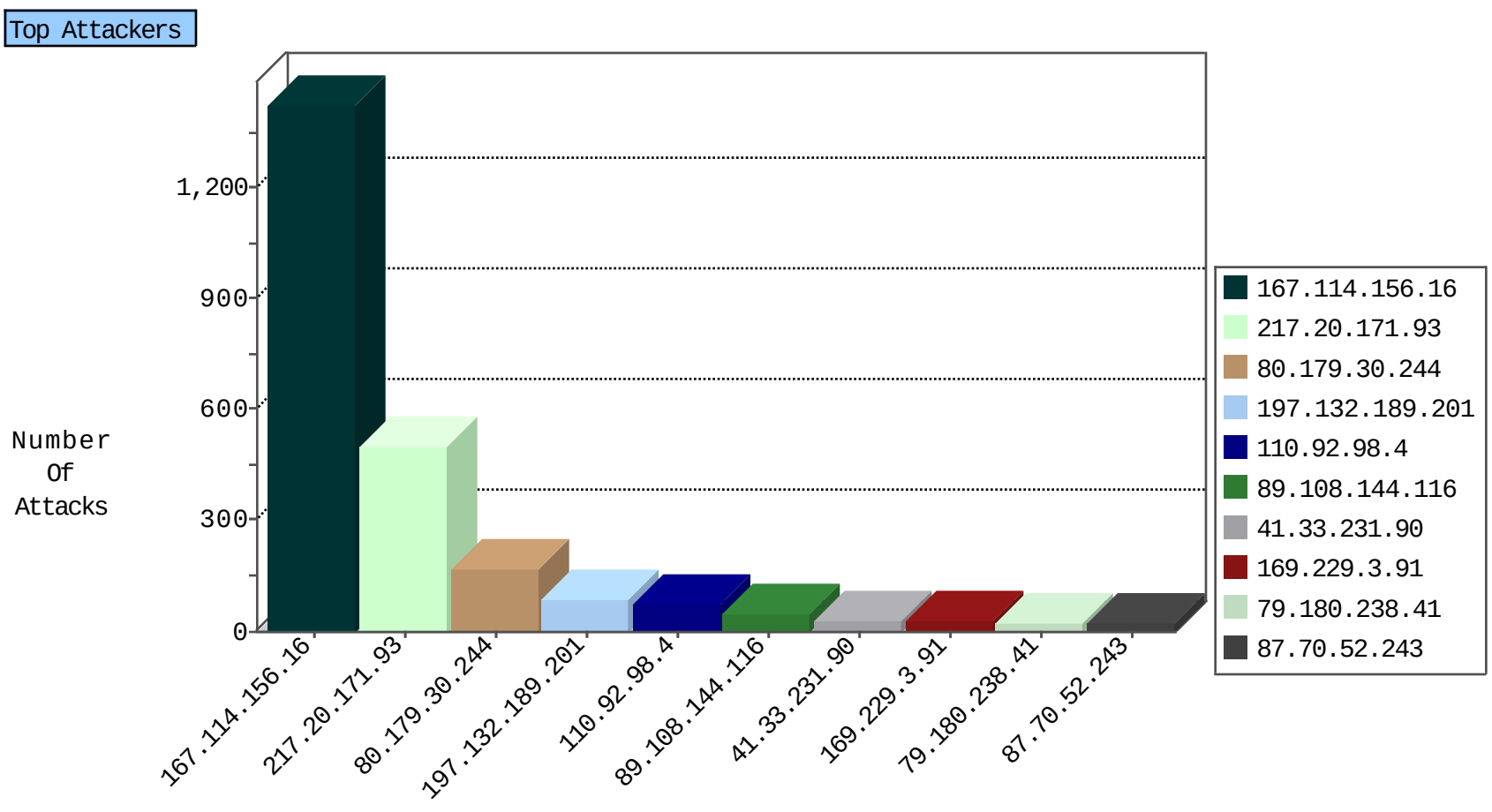
04-15-2016-11:04:06 to 04-15-2016-12:04:06

IDF Under Attack Daily Report



Top Target



Top Attackers

04-15-2016-11:04:06 to 04-15-2016-12:04:06

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	1428
79.178.217.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
204.42.253.2	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	2
101.201.147.32	China	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	2
123.59.59.52	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
94.102.52.10	Netherlands	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
82.145.218.209	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1

04-15-2016-11:04:06 to 04-15-2016-12:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.1.15	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.65.19.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
213.57.159.135	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.76	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-11:04:06 to 04-15-2016-12:04:06

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
82.205.126.170	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
80.82.78.38	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
198.144.184.120	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
184.168.75.231	147.237.77.226	United States	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
88.204.187.90	147.237.8.45	Kazakstan	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
88.204.187.90	147.237.8.45	Kazakstan	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
189.218.151.126	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.240.250.154	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.8.45	Kazakstan	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1

04-15-2016-11:04:06 to 04-15-2016-12:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.20.171.93	Ukraine	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	283
217.20.171.93	Ukraine	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	195
197.132.189.201	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
110.92.98.4	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.180.238.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
89.108.144.116	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
89.108.144.116	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
94.197.120.163	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.241.229.187	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
217.20.171.93	Ukraine	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.117.196.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
109.64.135.221	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.117.196.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
217.20.171.93	Ukraine	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.127.56.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.38.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.210.186.25	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.108.144.116	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.179.114.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.195.234	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.179.114.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
106.219.12.178	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.55.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.35.76.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.144.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.1.15	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
80.179.114.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.120.166.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.162.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
2.55.52.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.179.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.166.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.111.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.251	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.27.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.17.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.20.171.93	Ukraine	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3

04-15-2016-11:04:06 to 04-15-2016-12:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.182.195.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-15-2016-11:04:06 to 04-15-2016-12:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.179.30.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	172
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	19
2.53.63.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.164.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
2.55.36.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.6.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.148.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.39.15	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.19.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.33.77	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	2
80.179.114.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 80.179.114.3	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
157.55.39.251	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/gen...px	Block	1
23.81.235.55	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
109.64.247.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.46.13.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method [[#3]]‰Ò \¦)°HO6püv-_ì÷[[#18]]'Ç[[#5]]AB in URL	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
220.255.103.33	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
149.50.15.180	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.168.75.231	United States	147.237.77.226	www.chamatz.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.93.50	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in URL d¸i"¹¨[[λ#8«Þ]]ↄvmn¾ ƒ•	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
217.20.171.93	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 217.20.171.93	Block	1
109.66.0.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
207.46.13.129	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method šÖN[[#27]]hÂ`%°[[#30]],[[#26]]e)±ä\+ø[[#26]]x=ðøU#012•[[#28]]@![[#20]]+-•64nÉíÑ°þI[[#16]]¶ì[[#7]]÷ÚÛ•ö#012"pú%¸P*î	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-11039-he/dover.aspx	Block	1
84.94.181.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.112.235.59	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Malformed URL d¸i"¹¨[[λ#8«Þ]]ↄvmn¾ ƒ•	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Header Name	Block	1
40.77.167.84	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
217.20.171.93	Ukraine	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 217.20.171.93	Block	1
207.46.13.189	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.189	Block	1
110.86.186.223	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Unknown HTTP Request Method šÖN[[#27]]hÂ`%°[[#30]],[[#26]]e)±ä\+ø[[#26]]x=ðøU#012•[[#28]]@![[#20]]+-•64nÉíÑ°þI[[#16]]¶ì[[#7]]÷ÚÛ•ö#012"pú%¸P*î in URL	Block	1
80.179.114.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/69086.pdf	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/general.aspx	Block	1
157.55.39.15	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17615-en/dover.asp	Block	1
89.107.192.129	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
203.127.96.215	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-15-2016-11:04:06 to 04-15-2016-12:04:06