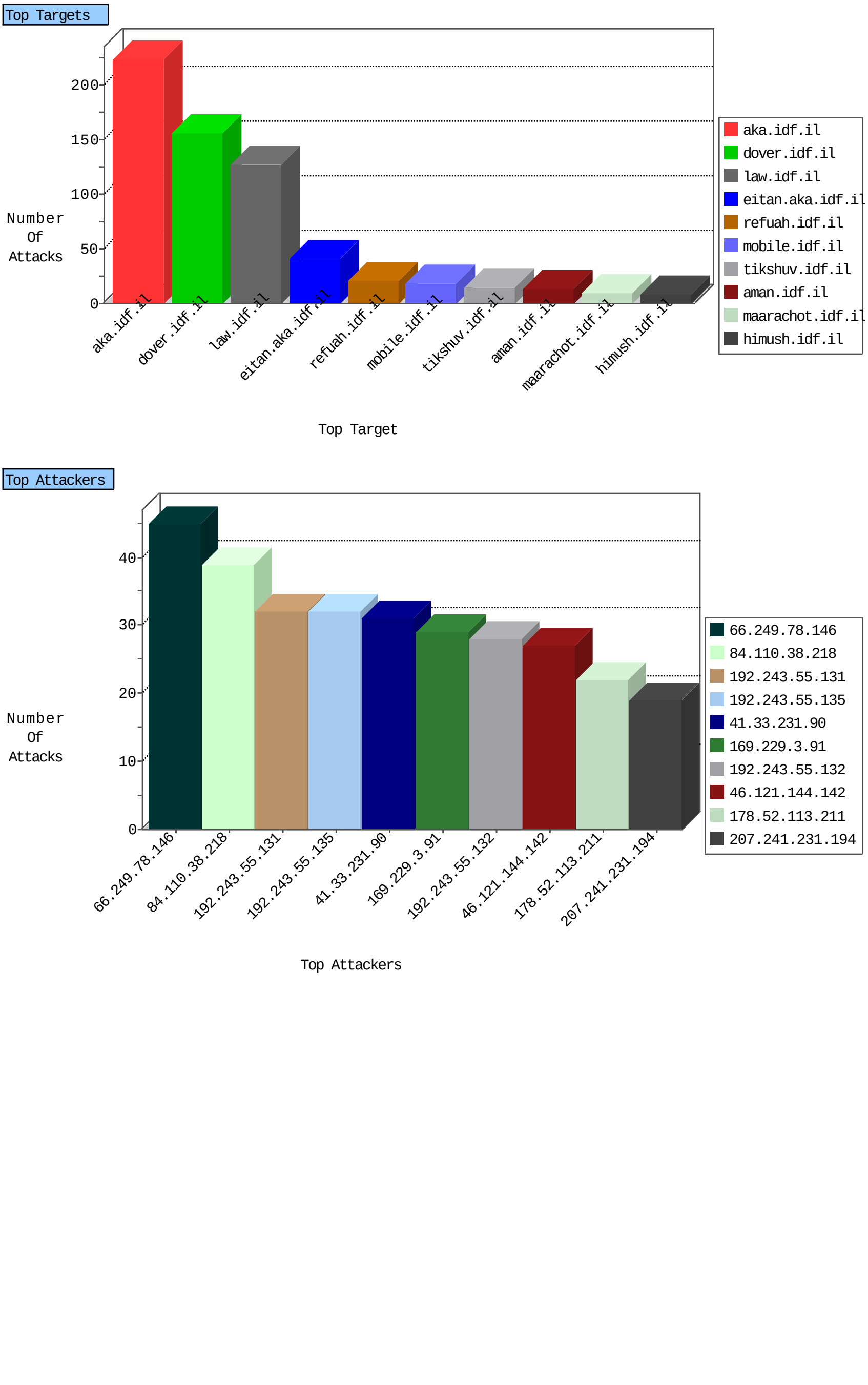
04-23-2016-16:04:00 to 04-23-2016-17:04:00

IDF Under Attack Daily Report



04-23-2016-16:04:00 to 04-23-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.202.139.239	Korea, Republic of	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-23-2016-16:04:00 to 04-23-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-16:04:00 to 04-23-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.102.9.101	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
87.70.32.236	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
40.114.42.13	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.76.42	Lithuania	refuah.idf.il	ET SCAN Potential SSH Scan	1
184.80.10.136	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
88.249.106.23	147.237.8.46	Turkey	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.76	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
184.80.10.136	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
184.80.10.136	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1

04-23-2016-16:04:00 to 04-23-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
84.110.38.218	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
178.52.113.211	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
81.218.125.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.154.37.235	Turkey	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
5.29.190.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.102.9.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
185.120.125.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.55.163.58	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
213.8.204.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
75.119.220.105	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
109.64.90.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.180.145.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.164.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
213.8.204.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.121.234.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.7	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
5.254.97.71	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.105.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
5.22.130.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.195.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.33.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.212.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
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
185.32.179.213	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.144.142	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.144.142	Block	27
84.94.188.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/links/mobile	Block	6
5.254.97.71	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.254.97.71	Block	3
5.254.97.71	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
87.70.115.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.188.47	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.94.188.47	Block	3
5.254.97.71	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/target.php	Block	2
109.64.172.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
123.59.59.52	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.mafengwo.cn/894-he/cogat.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Unknown HTTP Request Method Ã#0[[#30]]²óS°aËÕ•<ÜÏá0¿•EFL[[#3]]¥XF[[#28]]õuAoùG`<†È[[#6]]An')†Cí 7 in URL	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10035-en	Block	1
74.91.20.194	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Abnormally Long Request method	Block	1
14.202.185.28	Australia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
85.64.29.95	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/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	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
54.204.244.134	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in URL	Block	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
107.150.46.34	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
79.179.24.51	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Header Name	Block	1
37.26.149.147	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method ÅþX¸óë‘YÎÀ[[#16]]²:[[#1]]§Gÿi‰[[#22]]Žn[[#4]]€lïxn[k "ý±p‹?Á>ËRþòão>.[[#27]]µ¬äP}z_…—#012°OY•j	Block	1
87.70.105.97	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
107.150.46.38	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
79.179.24.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method Ã#0[[#30]]²óS°aËÕ•<ÜÏá0¿•EFL[[#3]]¥XF[[#28]]õuAoùG`<†È[[#6]]An')†Cí 7	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
46.4.22.136	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
130.185.155.74	Sweden	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Unknown HTTP Request Method ÅþX¸óë‘YÎÀ[[#16]]²:[[#1]]§Gÿi‰[[#22]]Žn[[#4]]€lïxn[k "ý±p‹?Á>ËRþòão>.[[#27]]µ¬äP}z_…—#012°OY•j in URL	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method ?Û¸ëÆ¨X!Œ]âßÀ$G?[[[#16]]m™ìõÝ+p[[#4]]ÈŽAì"~¶qA,õU4[[#2]]ÆV-A•5žå qÈ>ÄP[[#14]]²S in URL	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Malformed URL	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
46.117.17.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.17.41	Block	1
130.185.155.74	Sweden	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1

04-23-2016-16:04:00 to 04-23-2016-17:04:00