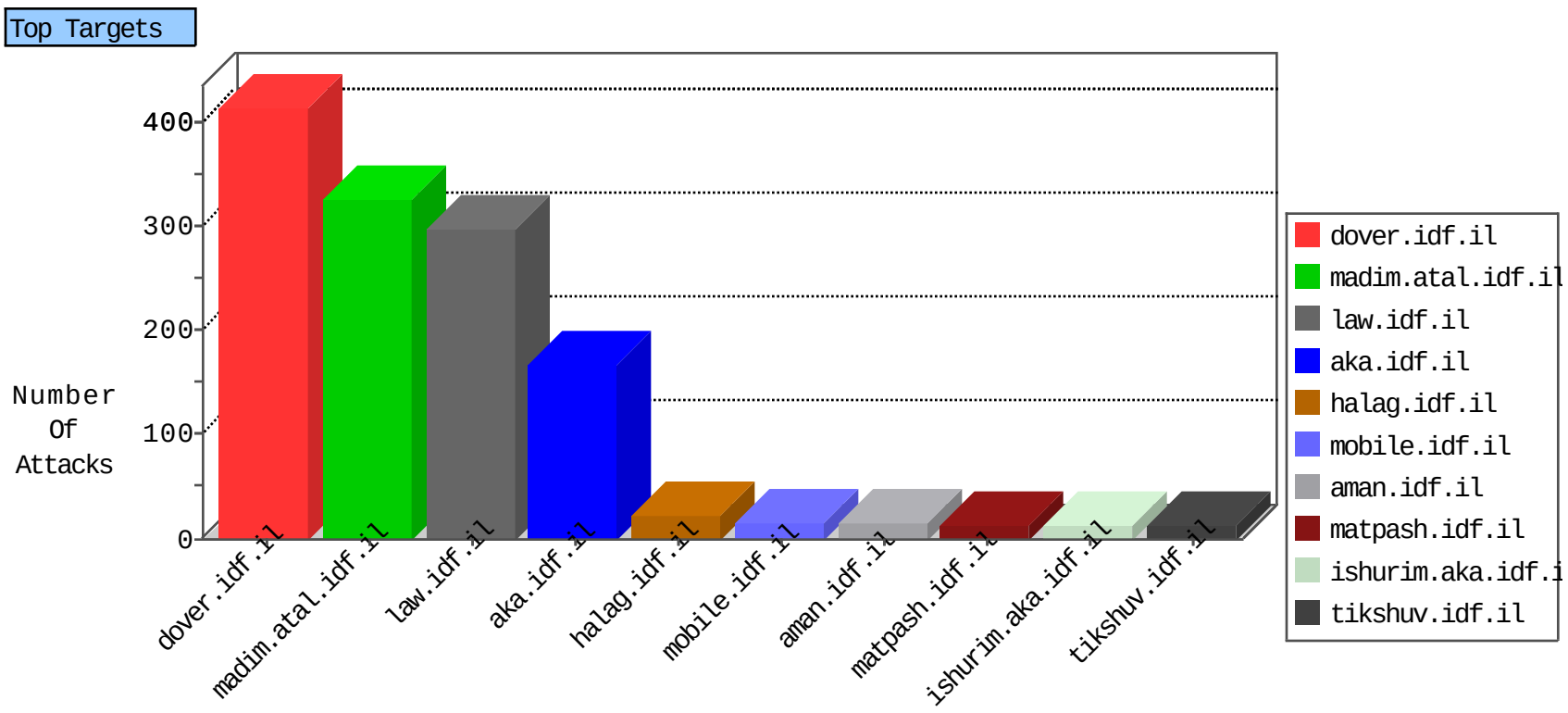
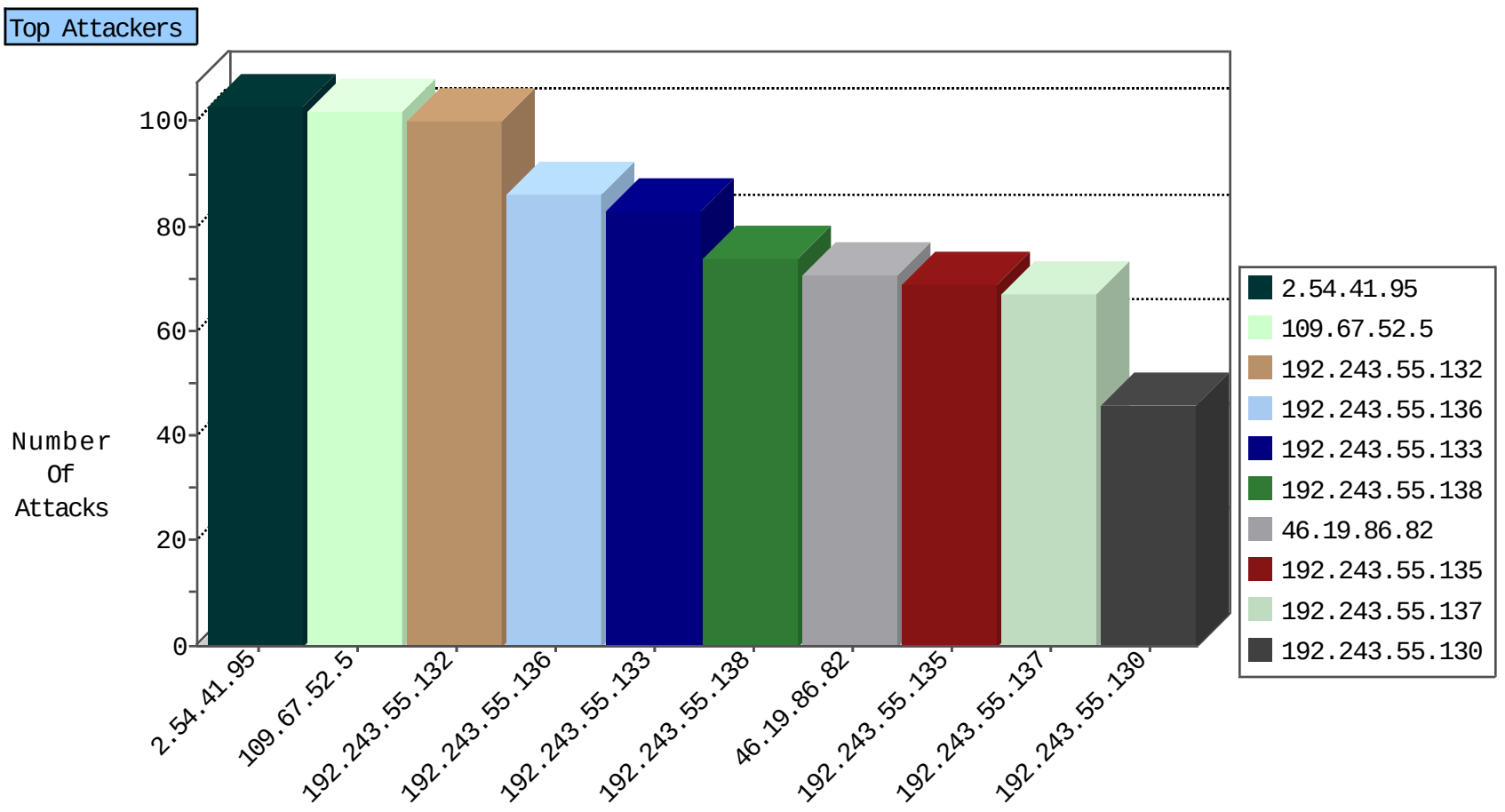
03-04-2016-09:04:08 to 03-04-2016-10:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.222.3	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
204.42.253.2	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
121.82.152.155	Japan	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.0.16	my-kosher-kravi.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
179.43.144.33	Switzerland	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.122	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.82	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.131.244	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
144.76.8.132	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.8.132	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
159.122.222.119	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
144.76.8.132	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.86.96	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
159.122.222.119	Netherlands	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
159.122.222.119	Netherlands	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
159.122.222.119	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
159.122.222.119	Netherlands	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
159.122.222.119	Netherlands	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
123.126.113.80	China	147.237.72.166	aka.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

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

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
212.224.109.175	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	1
159.122.222.119	147.237.0.19	Netherlands	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
159.122.222.119	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
159.122.222.119	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
109.253.156.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
213.57.100.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.52.24.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.52.184.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.132	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.136	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.147.186	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
88.253.1.211	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.41.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
109.67.52.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	71
79.181.220.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
46.19.86.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
2.52.23.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
50.62.160.145	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.62.160.145	Block	5
79.178.39.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.39.37	Block	4
2.52.150.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 83.14.142.130	Block	3
80.178.121.120	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 83.14.142.130	Block	2
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 83.14.142.130	Block	2
80.178.121.119	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.109.214.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Abnormally Long Header Line from 83.14.142.130	Block	2
176.228.44.128	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Malformed URL from 83.14.142.130	Block	2
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 83.14.142.130	Block	2
183.5.117.46	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
79.178.39.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 83.14.142.130	Block	2
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
1.55.96.48	Vietnam	147.237.76.86	navy.idf.il	Illegal Byte Code Character in URL d±[[#27]]"[[ך´¸‰½ף•#1א]] u[[#16]]hŒi6z¡![[#4]]¨ו5[[¿•#23µž]]ת×[[13#]]…Ùו-א´z[[#14]][[#8]]×‹ [k^l•ü¨qף·Ê-qcˆλpn6¼[[#28]]»v<va	Block	1
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper	Block	1
109.253.197.71	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
79.182.135.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Unknown HTTP Request Method íšîøÚ1šû[[#23]]d^ˆ._>‡k	Block	1
50.62.160.145	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
194.98.70.141	France	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
183.5.117.46	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 83.14.142.130 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 3	Block	1
1.55.96.48	Vietnam	147.237.76.86	navy.idf.il	Malformed URL d±[[#27]]"[[ך´¸‰½ף•#1א]]u[[#16]]hŒi6z¡![[#4]]¨ו 5•¿[[#23]]žµ[[ת#31Ù…]]λ-ıq¨ü•l^k[‹×]]8#[[]]41#[[z´ף^cq-Ê·λ pn6¼[[#28]]»v<va	Block	1
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdc0ns5kb2m=&infocenteritem=true	Block	1
157.55.39.58	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
80.82.65.82	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
83.43.157.237	Spain	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter pa in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	1
2.54.35.245	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.241.229.224	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdfצבא-הצלה	Block	1
183.5.117.46	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
79.178.39.37	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/klali.aspx	Block	1
109.67.52.5	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	NULL Character in Header Name at	Block	1
83.14.142.130	Poland	147.237.77.216	dover.idf.il	Malformed URL	Block	1
1.55.96.48	Vietnam	147.237.76.86	navy.idf.il	NULL Character in Method ,[[#0]][[#0]][[#0]]!lA€•?UÀÑ&J}^r×ô«[²ä+[[#0]]÷¥4q¼—™[[#28]][[#15]]•• ÷Ÿÿ”•;×»Èˆ˜	Block	1