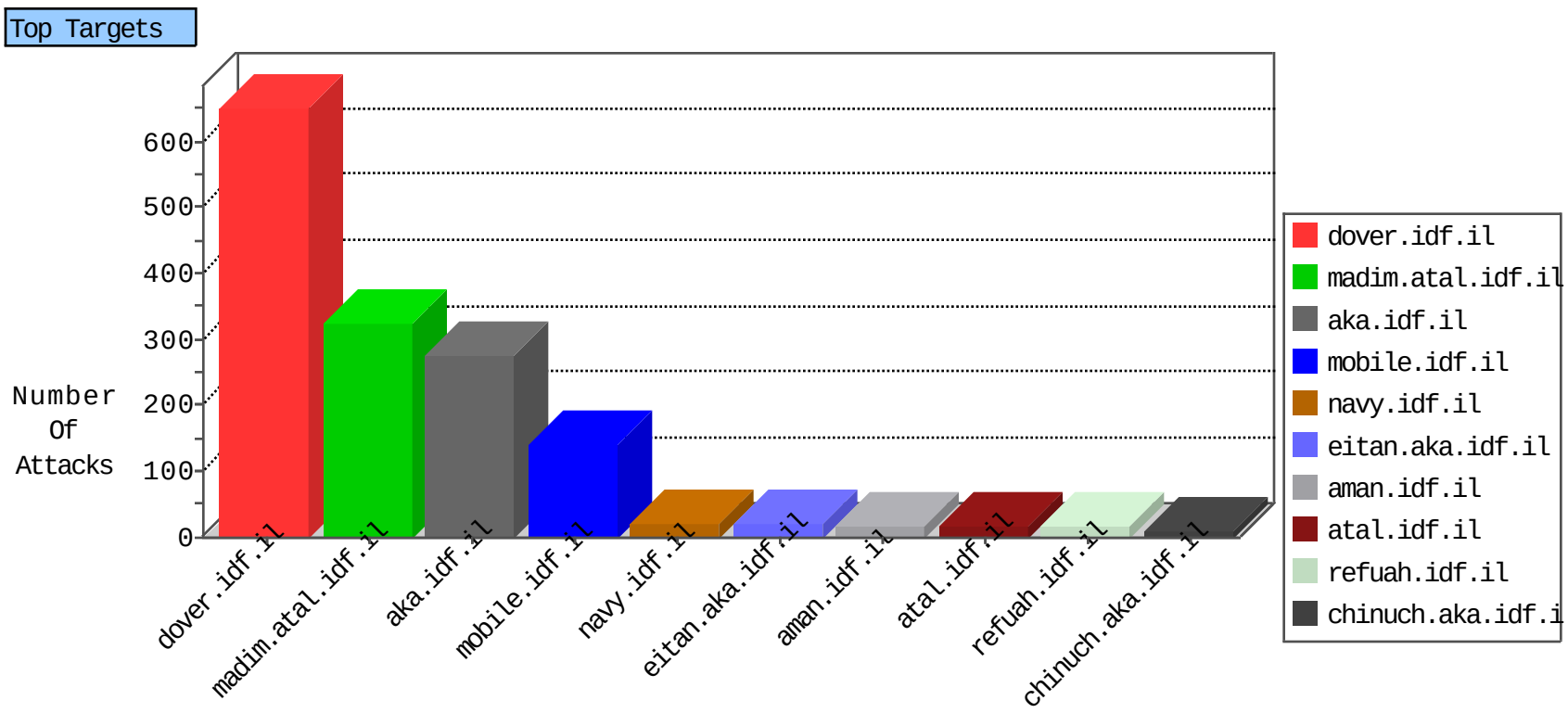
04-30-2016-19:04:08 to 04-30-2016-20:04:08

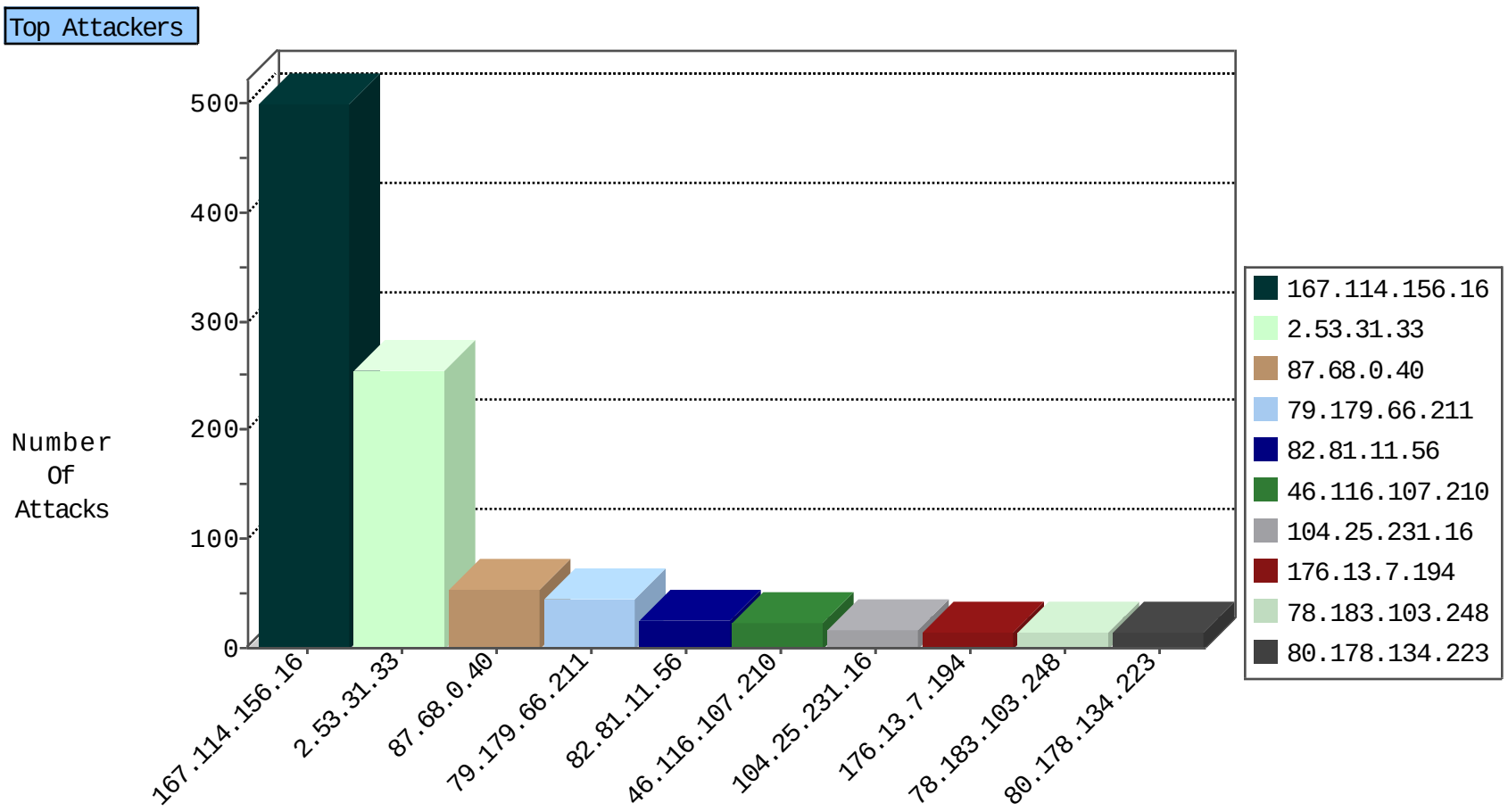
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-30-2016-19:04:08 to 04-30-2016-20:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	18161
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2405
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	4
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-30-2016-19:04:08 to 04-30-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-30-2016-19:04:08 to 04-30-2016-20:04:08

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	3
123.85.3.90	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
104.197.72.206	147.237.0.19	United States	madim.atal.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.175.172.235	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
40.76.60.52	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
123.85.3.90	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
78.183.103.248	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
59.175.172.235	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
40.76.60.52	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
40.76.60.52	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1

04-30-2016-19:04:08 to 04-30-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
82.81.11.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.116.107.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.110.109.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.7.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.178.134.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.21.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.253.208.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.216.97	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.26.149.230	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.210.187.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.176.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
196.113.59.182	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.108.136.204	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.65.72.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.79.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.90.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
217.132.16.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.146.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.1.129	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.94.174.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.111.152.232	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.242.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
132.75.167.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.159.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.160.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
104.25.231.16	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.13.16.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.152.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.148.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.160.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.120.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.134.171.219	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.175.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-30-2016-19:04:08 to 04-30-2016-20:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.183.218.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.81.209	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.178.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.220.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.50.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.134.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-30-2016-19:04:08 to 04-30-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.31.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	255
87.68.0.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
5.29.135.192	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	6
78.183.103.248	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 78.183.103.248	Block	5
82.81.11.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
78.183.103.248	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
85.64.21.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.116.107.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.64.179.233	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
78.183.103.248	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 78.183.103.248	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
176.13.7.194	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
31.210.187.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.179.66.211	Block	1
79.176.86.78	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
109.253.216.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
83.28.188.29	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_stor	Block	1
213.57.72.58	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.179.66.211	Block	1
149.78.236.148	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding |•₪¿¸%·fאא„b©ün¸¸–ynn'lš„[[#5]]v"(¢¸ p€[[#14]]„j" gk[[#23]][[#22]]•··‹[[#15]]bc²¦•[[#8]]hslz[[#28]]ž^bÿ3•o…¬¯[[#30]]•¶| •a¹[[#14]]Ýu¸#ˆ•[[#3]][[#19]][[-ɒɔ#5¸]]	Block	1
66.249.64.97	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/108889.pdf	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.179.66.211	Block	1
5.22.131.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
182.118.53.161	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name 3[[#24]]··'• in |•₪¿¸%·fאא„b©ünn–¸¸‹··•]]gk[[#23]][[#22"n'lš„[[#5]]v"(¢¸ p€[[#14]]„jר [[#15]]bc²¦•[[#8]]hslz[[#28]]ž^bÿ3•o…¬¯[[#30]]•¶|•a¹[[#14]]Ýu¸#ˆ•¸]]#5[[-ɒɔ]]#19[[]]#3[[	Block	1
113.174.239.250	Vietnam	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
85.64.17.152	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.149.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
216.245.215.102	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/wordpress/wp-admin/	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.179.66.211	Block	1
149.78.236.148	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.179.66.211	Block	1
87.70.108.70	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.182.14.50	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.179.66.211	Block	1
185.32.179.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
113.174.239.250	Vietnam	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Value at 11 for |•₪¿¸%·fאא„b©ün¸¸–ynn'lš„[[#5]]v"(¢¸ p€[[#14]]„j"gk[[#23]][[#22]]•··‹ [[#15]]bc²¦•[[#8]]hslz[[#28]]ž^bÿ3•o…¬¯[[#30]]•¶|•a¹[[#14]]Ýu¸#ˆ•¸]]#5[[-ɒɔ]]#19[[]]#3[[	Block	1
68.65.120.171	United States	147.237.0.19	madim.atal.idf.i	Multiple Unauthorized URL Access from 68.65.120.171	Block	1
46.19.86.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 79.179.66.211	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.179.66.211	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.179.66.211	Block	1
95.185.114.55	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
80.178.6.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1

04-30-2016-19:04:08 to 04-30-2016-20:04:08