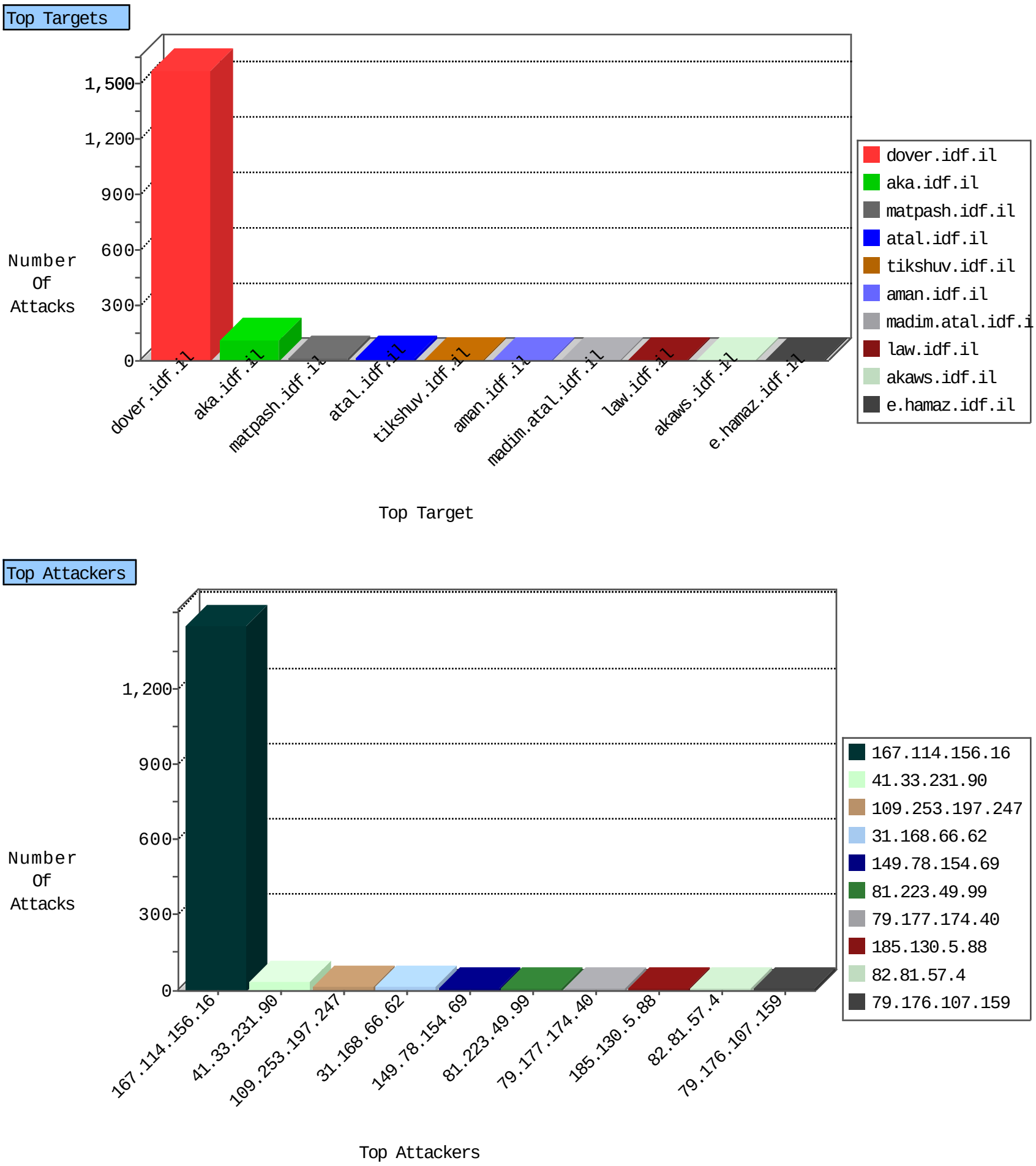
04-15-2016-08:04:02 to 04-15-2016-09:04:02

IDF Under Attack
Daily Report



04-15-2016-08:04:02 to 04-15-2016-09:04:02

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	1451
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	4
81.223.49.99	Austria	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Http	drop	1
94.102.52.10	Netherlands	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.16	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
81.223.49.99	Austria	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Http	drop	1
209.126.127.16	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
81.223.49.99	Austria	147.237.76.200	eitan.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
216.218.206.83	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
81.223.49.99	Austria	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
209.126.127.16	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1

04-15-2016-08:04:02 to 04-15-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
173.234.159.250	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
178.137.90.202	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3
37.26.148.155	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.201.89	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.201.89	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.201.89	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	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
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-15-2016-08:04:02 to 04-15-2016-09:04:02

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
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
200.195.135.82	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -f -sS	1
195.154.54.169	147.237.77.74	France	law.idf.il	ET SCAN NMAP -sS window 1024	1
87.229.116.42	147.237.0.35	Hungary	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.77.243	Lithuania	mobile.idf.il	ET SCAN Potential SSH Scan	1
37.97.143.205	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.88	147.237.77.227	Lithuania	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.77.212	Lithuania	e.dover.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.77.121	Lithuania	e.navy.idf.il	ET SCAN Potential SSH Scan	1
173.65.154.27	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
112.203.215.95	147.237.76.31	Philippines	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
200.195.135.82	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.77.205	Japan	prisha.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.77.234	Lithuania	halag.idf.il	ET SCAN Potential SSH Scan	1
37.97.143.205	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.77.226	Lithuania	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.77.170	Lithuania	maarachot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.8.28	Lithuania	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
122.117.163.144	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-15-2016-08:04:02 to 04-15-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.253.197.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.179.22.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.224.168	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.81.57.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.174.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.174.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
118.151.157.17	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.31.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.35.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.147.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.161.116.98	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.180.130.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.57.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
138.134.192.10	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
5.22.130.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.202.239.134	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.218.55.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
195.76.232.154	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
157.55.39.98	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
118.193.163.150	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
74.82.47.8	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
200.74.240.180	Panama	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.168.170.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.70.198	Netherlands	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
120.132.84.59	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.70.89.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
38.229.1.15	United States	147.237.0.33	idf.il	drop		drop	1
81.223.49.99	Austria	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.246	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.70.198	Netherlands	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.11	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.226.240	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.251.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
200.74.240.180	Panama	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.210.188.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.230.223.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

04-15-2016-08:04:02 to 04-15-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
219.74.180.192	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.47.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.226.159.130	Germany	147.237.76.86	navy.idf.il	Suspicious Response Code	Block	2
120.132.50.135	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.qyer.com/894-he/atal.aspx	Block	1
80.230.223.206	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Tú	Block	1
203.127.58.231	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.153.93	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
112.134.80.217	Sri Lanka	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.176.107.159	Block	1
54.165.3.60	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/-	Block	1
138.134.192.10	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
80.230.223.227	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	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
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
112.134.80.217	Sri Lanka	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.176.107.159	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71706.pdf	Block	1
141.8.184.11	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
81.223.49.99	Austria	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /	Block	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL '“z/0-;[[#21]]³¯[w¡¼ƛ1iyyn.ü ü[[#4]][[#23]]t[[#12]]¦´¼[[#26]][[#28]]u[[¬#31isÝ]]ƛ´0cÙjžü§~Ýj &ÐÐ"v·"¢¸l¢ ,7bŽŸj´¦]]#8[[2´Œ6"	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
40.77.167.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
118.193.163.150	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Tú	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-en/idfgdover.aspx	Block	1
157.55.39.27	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
87.70.85.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.176.107.159	Block	1
212.76.105.181	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
52.23.219.181	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1930-en/-	Block	1
119.73.253.4	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.230.223.106	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.3.239	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
79.176.107.159	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.176.107.159	Block	1
219.74.148.111	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.165.3.60	United States	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../images/shared/home.png	Block	1

04-15-2016-08:04:02 to 04-15-2016-09:04:02