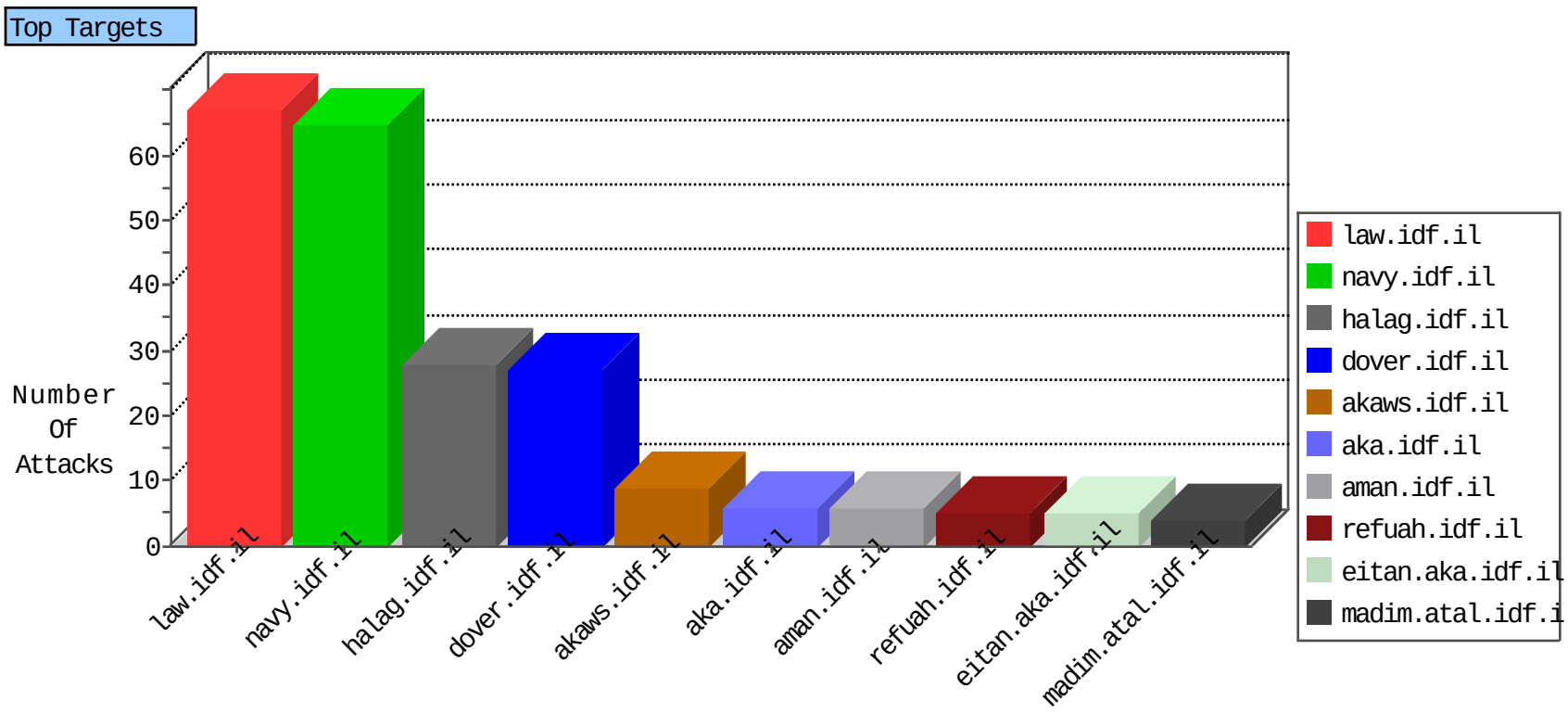
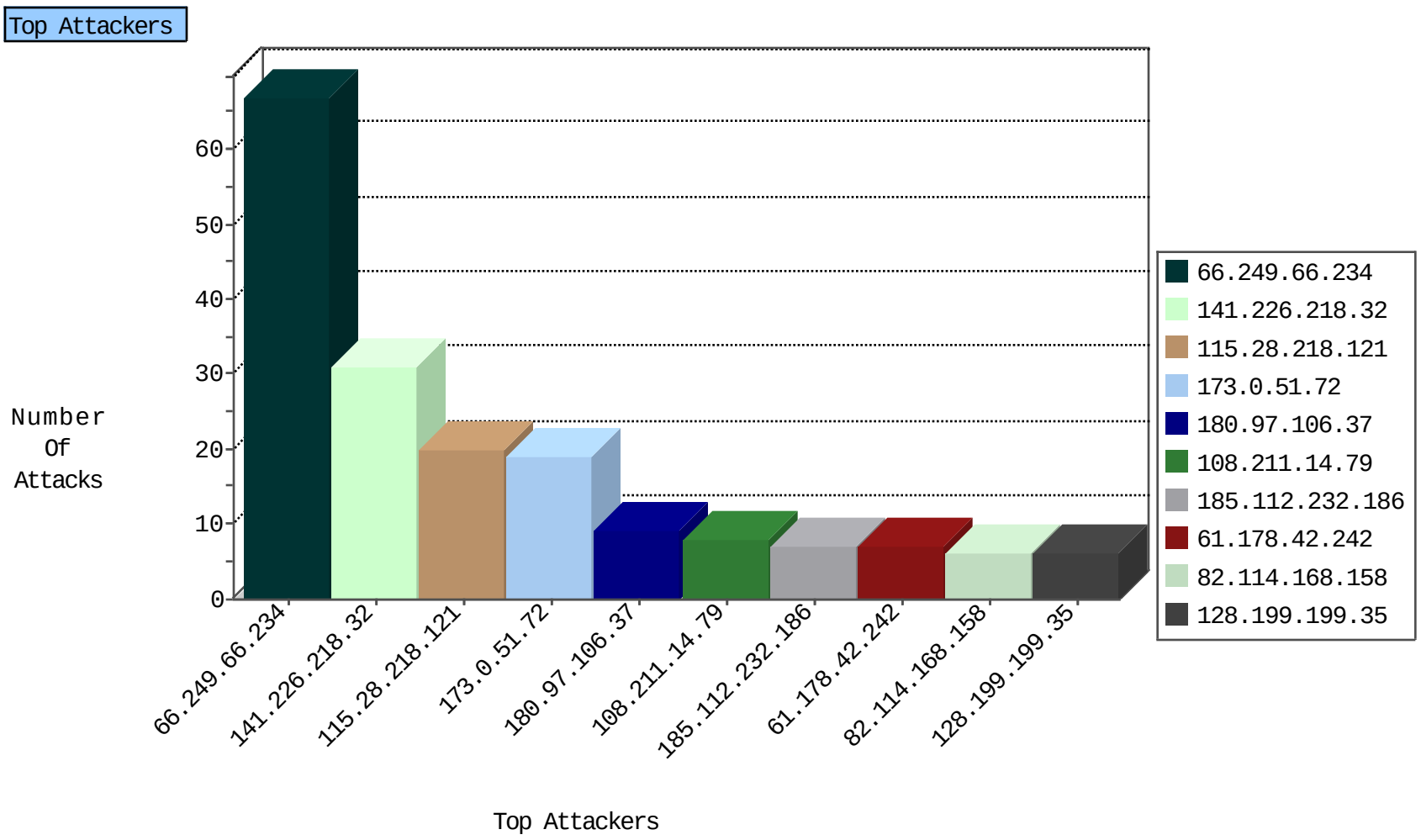
09-22-2016-05:04:05 to 09-22-2016-06:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-22-2016-05:04:05 to 09-22-2016-06:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.81.157.152	France	147.237.76.44	e.refuah.idf.il	Black List	drop	1
185.81.157.161	France	147.237.76.177	ncore.idf.il	Black List	drop	1
185.81.157.152	France	147.237.76.30	himush.idf.il	Black List	drop	1

09-22-2016-05:04:05 to 09-22-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.100	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.100	United States	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
89.161.141.186	Poland	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
128.199.199.35	Singapore	147.237.76.86	navy.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

09-22-2016-05:04:05 to 09-22-2016-06:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.234	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	67
61.178.42.242	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.200	United States	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
61.178.42.242	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
61.178.42.242	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
163.172.213.241	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.126.231.44	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.199.199.35	147.237.76.86	Singapore	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.183.223.228	147.237.77.19	Latvia	law-forum.idf.il	ET SCAN Potential SSH Scan	1
82.208.160.181	147.237.77.216	Romania	dover.idf.il	Tehila - Perl LWP with fake user agent	1
41.160.222.18	147.237.77.205	South Africa	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
80.15.154.133	147.237.76.30	France	himush.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.168.128	147.237.76.86	Canada	navy.idf.il	ET SCAN Potential SSH Scan	1
61.178.42.242	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
198.167.136.153	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.178.42.242	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.93.185.10	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.178.42.242	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.178.42.242	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
163.172.213.241	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.77.61	Latvia	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
110.5.109.236	147.237.8.27	Indonesia	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
41.160.222.18	147.237.77.227	South Africa	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
80.15.154.133	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.168.128	147.237.0.35	Canada	akaws.idf.il	ET SCAN Potential SSH Scan	1

09-22-2016-05:04:05 to 09-22-2016-06:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
108.211.14.79	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
115.28.218.121	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
50.83.246.154	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.112.232.186	Iraq	147.237.0.35	akaws.idf.il	drop	First packet isn't SYN	drop	5
82.114.168.158	Yemen	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
115.28.218.121	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
115.28.218.121	China	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
115.28.218.121	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
141.226.218.32	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	3
115.28.218.121	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	3
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
54.167.185.106	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.29.162.42	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.218.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
185.112.232.186	Iraq	147.237.0.35	akaws.idf.il	drop		drop	2
173.0.51.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence		monitor	2
46.19.85.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
129.10.9.120	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.186.113.169	Japan	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.107	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
180.97.106.37	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
46.19.85.161	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
173.0.51.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
139.162.37.147	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.119	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
100.13.130.4	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
141.226.218.32	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
110.5.109.236	Indonesia	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.123	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.18	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
100.13.130.4	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.71	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
82.114.168.158	Yemen	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
174.61.8.106	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.80	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
171.120.26.143	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
119.81.249.133	Hong Kong	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
104.243.163.114	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-22-2016-05:04:05 to 09-22-2016-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	4
128.199.199.35	Singapore	147.237.76.86	navy.idf.il	Parameter Type Violation docId in navy.idf.il/navy/general.aspx	Block	3
180.97.106.37	China	147.237.76.86	navy.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
198.98.124.221	United States	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1
89.161.141.186	Poland	147.237.76.86	navy.idf.il	Parameter Type Violation catId in navy.idf.il/navy/general.aspx	Block	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.161	Block	1
141.226.218.32	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.124.37.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
198.98.124.221	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/blogs/wp-login.php	Block	1
180.97.106.37	China	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
103.199.117.3	India	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter UncleTypesToIgnore	Block	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	Multiple NULL Character in Method from 180.97.106.161	Block	1
144.76.120.23	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
81.169.144.135	Germany	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter catId	Block	1
207.46.13.86	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
180.97.106.37	China	147.237.72.156	aman.idf.il	Multiple NULL Character in Method from 180.97.106.37	Block	1
103.199.117.3	India	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
180.97.106.161	China	147.237.76.42	refuah.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
176.14.244.114	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
81.169.144.135	Germany	147.237.76.86	navy.idf.il	Distributed Parameter Type Violation on navy.idf.il/navy/general.aspx parameter docId	Block	1
180.97.106.37	China	147.237.76.86	navy.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
128.199.199.35	Singapore	147.237.76.86	navy.idf.il	Parameter Type Violation UncleTypesToIgnore in navy.idf.il/navy/general.aspx	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/76/	Block	1
180.97.106.161	China	147.237.76.42	refuah.idf.il	Distributed NULL Character in Method	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
89.161.141.186	Poland	147.237.76.86	navy.idf.il	Parameter Type Violation UpperCatId in navy.idf.il/navy/general.aspx	Block	1

09-22-2016-05:04:05 to 09-22-2016-06:04:05