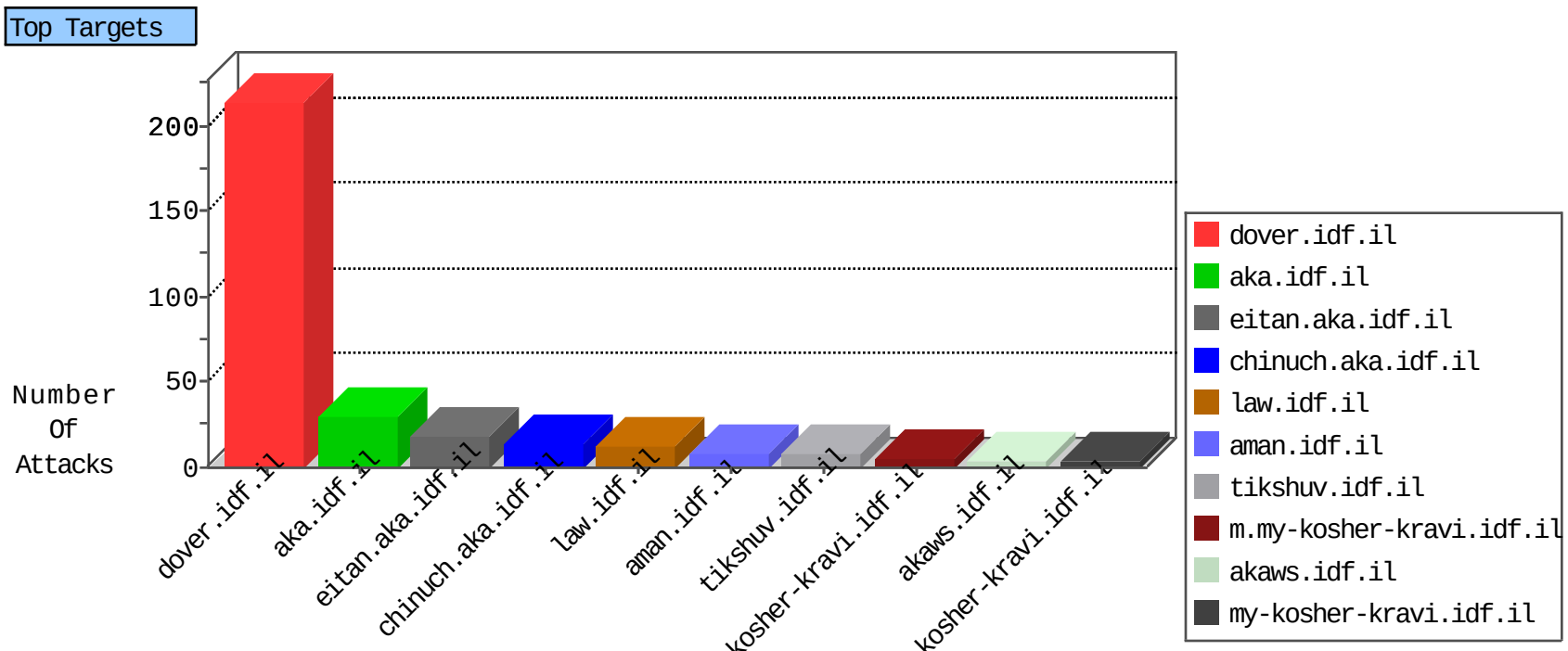
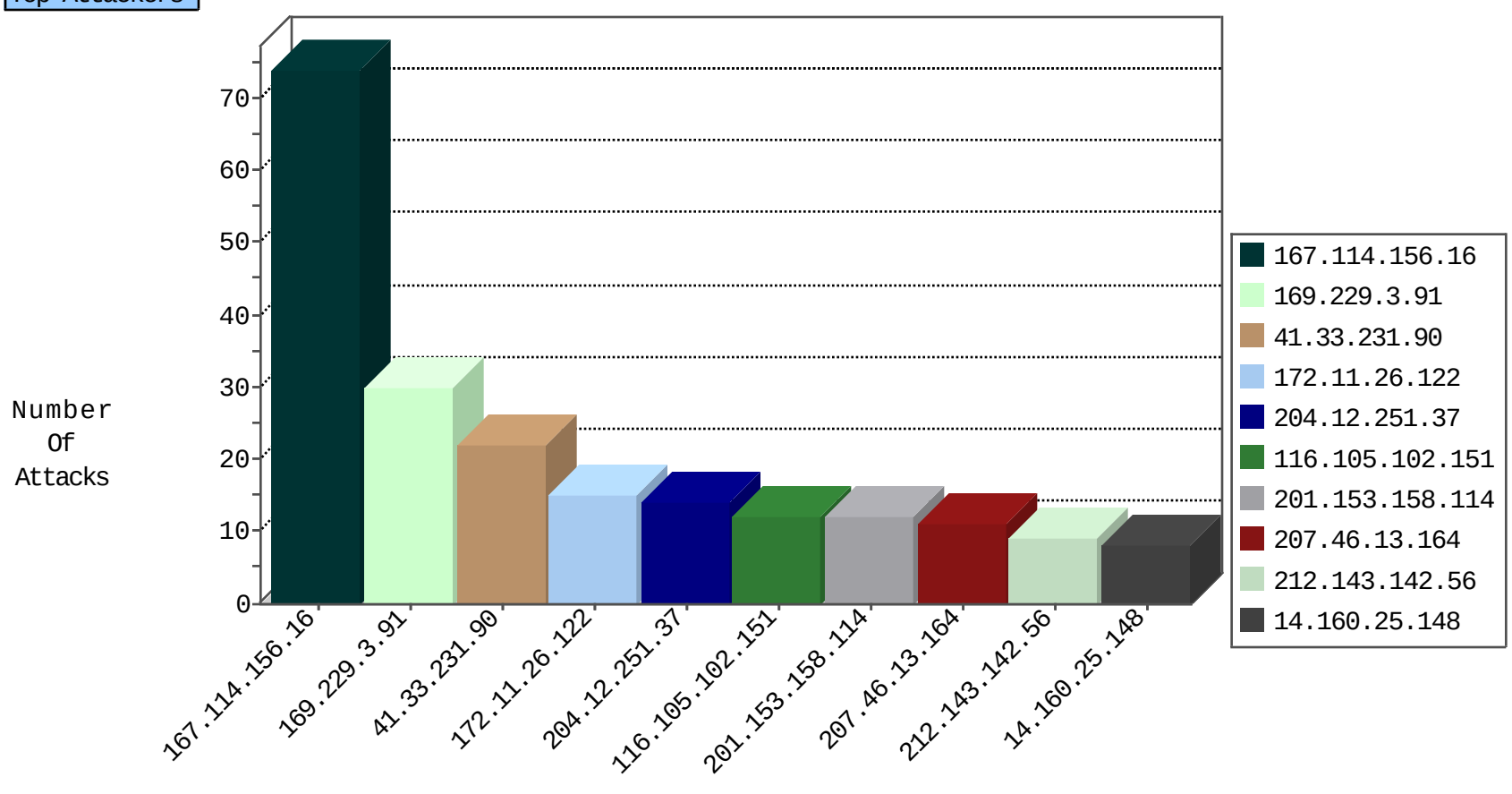
12-29-2015-04:04:01 to 12-29-2015-05:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-29-2015-04:04:01 to 12-29-2015-05:04:01

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	DOS-Tool-SwitchbladG	dest-reset	1765
66.249.66.125	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	38
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
162.213.153.152	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

12-29-2015-04:04:01 to 12-29-2015-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-29-2015-04:04:01 to 12-29-2015-05:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
151.217.178.88	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
88.249.106.23	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.53.128.60	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.204.188.142	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 3072	1
5.39.222.253	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
195.22.126.20	147.237.76.201	Poland	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.76.197		e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-29-2015-04:04:01 to 12-29-2015-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
172.11.26.122	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
204.12.251.37	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
207.46.13.164	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
14.160.25.148	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
116.105.102.151	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
201.153.158.114	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
116.105.102.151	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
70.197.195.230	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
82.145.219.64	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
14.162.183.105	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
75.13.5.111	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
201.153.158.114	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
201.153.158.114	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
130.193.51.104	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.198	United States	147.237.0.35	akaws.idf.il	drop		drop	1
204.12.251.37	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.122	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
88.81.59.12	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.42	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.96	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.123	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.172.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.73.127.69	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.86	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
78.46.97.213	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
52.90.147.70	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.200	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
40.77.167.105	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.112	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
184.105.139.122	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.167.162	Netherlands	147.237.0.33	idf.il	drop	SAM rule	drop	1
172.11.26.122	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.50	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
162.216.46.122	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.114	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.194	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.150.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

12-29-2015-04:04:01 to 12-29-2015-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.161.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.253.128.124	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
141.8.142.82	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
188.42.240.119	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-he/modules/forums/forum.aspx	Block	1
120.52.73.12	China	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1393-en/dover.aspx	Block	1
98.202.206.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Malformed URL q>pâ€¡[[#11]]b1Â¾â€¡Â¿hÂ?Â§Ã·×ž[[#27]]Ëœ[[#8]]Æ'[[#3]]×?[[#29]]a[[#0]]6hÖ¸×?[[#11]]Ö³.ÃžÂœo×€uÂ¥vb[[[#15]]	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
141.212.122.192	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
207.46.13.164	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	NULL Character in Method	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	NULL Character in Method [[#4]]\ÃºÂ¬Ã¼[[#0]]1Ã?Ã˜[[#2]]U?Ã»Â£[[#5]]S-Ã¼Â¨Ã˜[[#2]]Â´Â²[[#8]]Â¸Â±>Ãš}Â,Â®IX[[#8]]Â¹ÃµÃºÂ¦Â¶hÃ½Â«Â,8Â¡BÂ¶9	Block	1
80.246.136.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.246	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method ÑŠ in URL	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
120.52.73.22	China	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/901-en/cogat.aspx	Block	1
104.245.98.5		147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/cgi-bin/php	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.66.34	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
176.13.8.89	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Unknown HTTP Request Method [[#4]]\ÃºÂ¬Ã¼[[#0]]1Ã?Ã˜[[#2]]U?Ã»Â£[[#5]]S-Ã¼Â¨Ã˜[[#2]]Â´Â²[[#8]]Â¸Â±>Ãš}Â,Â®IX[[#8]]Â¹ÃµÃºÂ¦Â¶hÃ½Â«Â,8Â¡BÂ¶9 in URL	Block	1
85.250.177.203	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.187.56.47	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL Ö´&ÃŠ[[#11]]â€ºbÂ»vav1Â£[[#5]]08d×²Ö²7%(Â?[[#24]]3j×?	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
120.52.73.25	China	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1393-en/dover.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	NULL Character in URL q>pâ€¡[[#11]]b1Â¾â€¡Â¿hÂ?Â§Ã·×ž[[#27]]Ëœ[[#8]]Æ'[[#3]]×?[[#29]]a[[#0]]6hÖ¸×?[[#11]]Ö³.ÃžÂœo×€uÂ¥vb[[[#15]]	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Header Name	Block	1
176.13.11.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
117.177.250.146	China	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Query String on q>pâ€¡[[#11]]b1Â¾â€¡Â¿hÂ?Â§Ã·×ž[[#27]]Ëœ[[#8]]Æ'[[#3]]×?[[#29]]a[[#0]]6hÖ¸×?[[#11]]Ö³.ÃžÂœo×€uÂ¥vb[[[#15]]	Block	1
89.138.201.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.1	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal URL Path Encoding Ö´&ÃŠ[[#11]]â€ºbÂ»vav1Â£[[#5]]08d×²Ö²7%(Â?[[#24]]3j×?	Block	1
141.8.142.65	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method Â?Ã¶ÂŽÃ?Â²[[#1]]VÂµH[[#20]]ÂŸÃ˜~ in URL q>pâ€¡[[#11]]b1Â¾â€¡Â¿hÂ?Â§Ã·×ž[[#27]]Ëœ[[#8]]Æ'[[#3]]×?[[#29]]a[[#0]]6hÖ¸×?[[#11]]Ö³.ÃžÂœo×€uÂ¥vb[[[#15]]	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Abnormally Long Request method	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1756	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
180.76.15.29	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

12-29-2015-04:04:01 to 12-29-2015-05:04:01