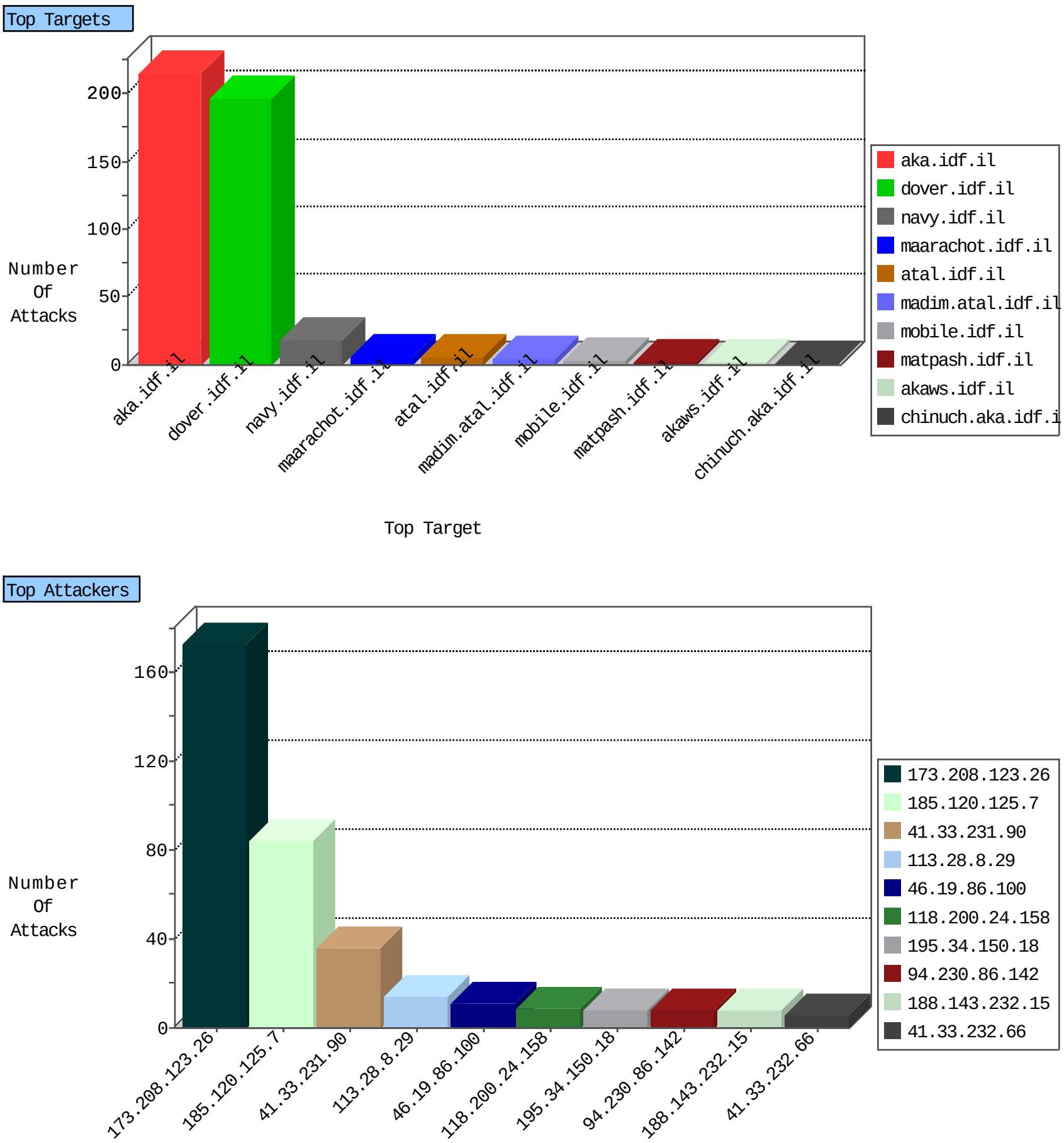
02-01-2016-04:04:02 to 02-01-2016-05:04:02

IDF Under Attack Daily Report



02-01-2016-04:04:02 to 02-01-2016-05:04:02

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	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
89.248.174.4	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
184.26.160.64	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
70.192.196.31	United States	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	1
184.26.160.64	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.59	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1

02-01-2016-04:04:02 to 02-01-2016-05:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
38.87.46.138	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2

02-01-2016-04:04:02 to 02-01-2016-05:04:02

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
222.186.42.206	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.206	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.69.53.105	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
130.211.93.253	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.206	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
162.243.64.165	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
95.109.126.154	147.237.76.30	Sweden	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-01-2016-04:04:02 to 02-01-2016-05:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.208.123.26	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	135
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
113.28.8.29	Hong Kong	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
173.208.123.26	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
118.200.24.158	Singapore	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.78.154	United States	147.237.76.86	navy.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
66.249.78.161	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
76.115.96.90	United States	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
94.230.86.142	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
70.199.69.54	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.32.179.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.199.69.54	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.132.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
123.125.71.57	China	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.6.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.126	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.154.155.27	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.7	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
187.178.228.228	Mexico	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.230.86.142	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
31.210.186.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.239	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.124	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.95.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
173.208.213.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
123.125.71.57	China	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
87.69.95.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.95	United States	147.237.0.35	akaws.idf.il	drop		drop	1
70.210.158.27	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 173.208.123.26 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	3
76.115.96.90	United States	147.237.77.170	maarachot.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	2
5.29.50.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	2
173.208.123.26	United States	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
69.162.139.9	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name ÂŸ Ö·YÂ¥[[#28]]Ã·Â¯~oÃ·×´[[#4]]×›;Â¡Â¥6×³ in ×šÃœ +Ö¹[[#22]][[#22]]ck×?[[#30]]â€¦â„¢Â¥<kuâ€¦kÂ½Ã·Â¹ÂžÂ¯	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
188.143.232.15	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/900-en/	Block	1
40.77.167.35	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Malformed URL ×šÃœ+Ö¹[[#22]][[#22]]ck×?[[#30]]â€¦â„¢Â¥<kuâ€ ¦kÂ½Ã·Â¹ÂžÂ¯	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Too Many Headers per Request - 42 Headers	Block	1
70.210.158.27	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String ÂŸ Ö·YÂ¥[[#28]]Ã·Â¯~oÃ·×´[[#4]]×›;Â¡Â¥6×³ on ×šÃœ +Ö¹[[#22]][[#22]]ck×?[[#30]]â€¦â„¢Â¥<kuâ€¦kÂ½Ã·Â¹ÂžÂ¯	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
40.77.167.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name EÃ˜qXÂ¬Â³fÂŠ R"Ã¾/Ã§nÂ¾[[#5]][[#12]]Â‡ÃŠÃ™[[#0]][[#21]]QÂ‡Ã†HÃ¡Â›&Ã«PÂ' Ã·Â·[[#11]]Ã¹Ã–Ã²Ã¥~Â¤WÂªÃ»Ã†Ã¨Ã´Â¨Â”(Â˜Â°Â¸Ã§LÂ¥Ã¾5"ÃŽ Ã?[[#16]]+Â?Ã'pÃ¶Â¤Ã½EXÂ·Â'Â‡Ã˜[[#1]]iÂ¾Ã?[[#1]]Ã³Ã¶9Â²Ã‰Ã^ [[#7]]Ã˜_Ã?Â¹+ÃªÃ”Ã-gÂ·Â˜Â€AA[[#18]]Â Ã¹!cÂ®Â®9Ms	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ÂžÂ¹Â?-Ã?4[[#30]]ÂŽÃ§Â?Â?Â“	Block	1
76.18.213.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL ×šÃœ+Ö¹[[#22]][[#22]]ck×?[[#30]]â€¦â„¢Â¥<kuâ€¦kÂ½Ã·Â¹ÂžÂ¯	Block	1
113.28.8.29	Hong Kong	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	NULL Character in Header Name at EÃ˜qXÂ¬Â³fÂŠ R"Ã¾/Ã§nÂ¾[[#5]][[#12]]Â‡ÃŠÃ™[[#0]][[#21]]QÂ‡Ã†HÃ¡Â›&Ã«PÂ' Ã·Â·[[#11]]Ã¹Ã–Ã²Ã¥~Â¤WÂªÃ»Ã†Ã¨Ã´Â¨Â”(Â˜Â°Â¸Ã§LÂ¥Ã¾5"ÃŽ Ã?[[#16]]+Â?Ã'pÃ¶Â¤Ã½EXÂ·Â'Â‡Ã˜[[#1]]iÂ¾Ã?[[#1]]Ã³Ã¶9Â²Ã‰Ã^ [[#7]]Ã˜_Ã?Â¹+ÃªÃ”Ã-gÂ·Â˜Â€AA[[#18]]Â Ã¹!cÂ®Â®9Ms	Block	1
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/metaemmeetheadknesiyot.aspx	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
185.120.126.39		147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-he/	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Malformed URL from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
122.107.118.54	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	NULL Character in Method ÂžÂ¹Â?-Ã?4[[#30]]ÂŽÃ§Â?Â?Â“	Block	1
66.249.65.131	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/638.pdf	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ÂžÂ¹Â?-Ã?4[[#30]]ÂŽÃ§Â?Â?Â“	Block	1
94.230.86.142	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 173.208.123.26	Block	1
173.208.123.26	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 20	Block	1