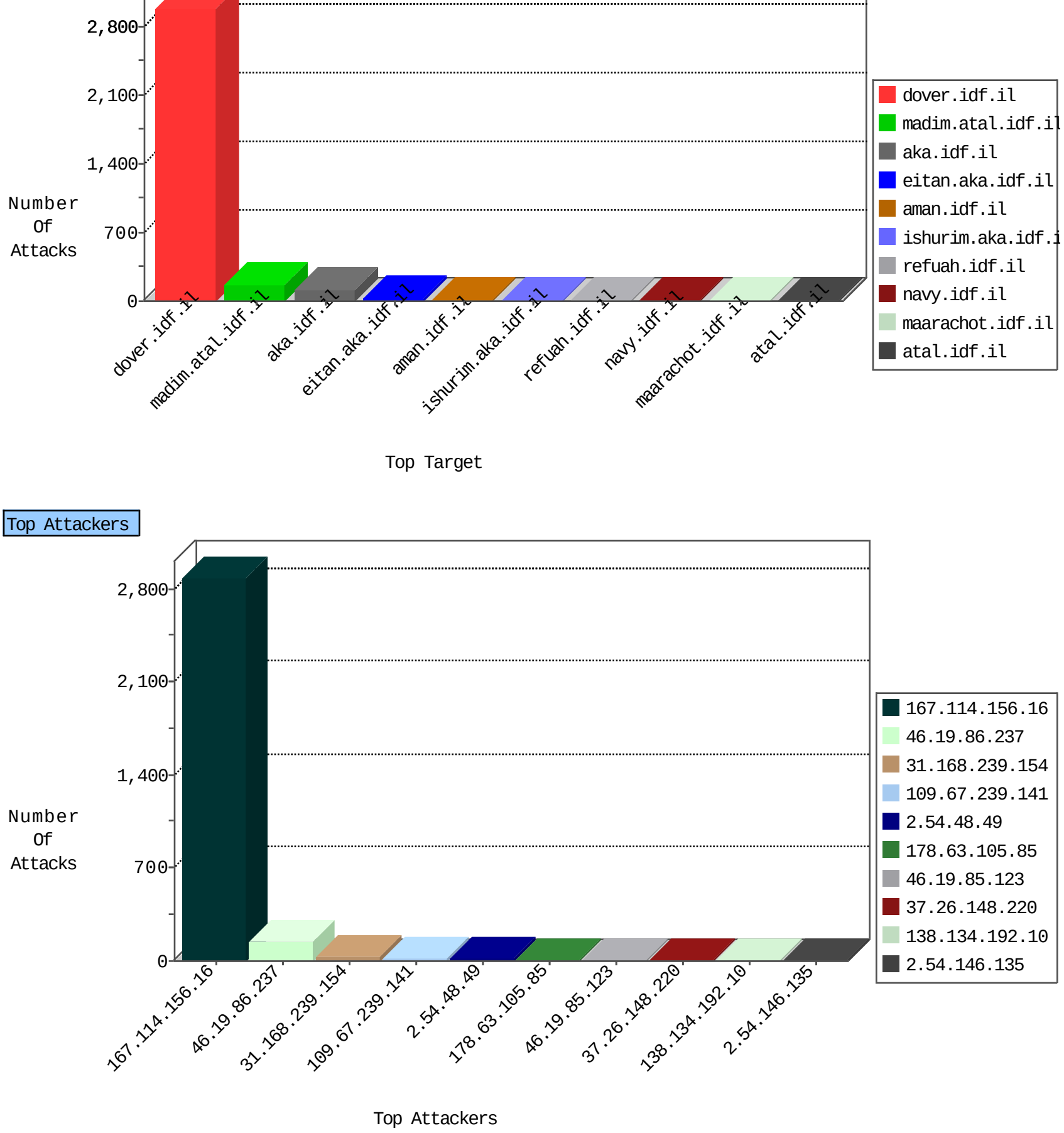
03-14-2016-07:04:03 to 03-14-2016-08:04:03

IDF Under Attack Daily Report



03-14-2016-07:04:03 to 03-14-2016-08:04:03

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	3775
37.26.148.220	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	2

03-14-2016-07:04:03 to 03-14-2016-08:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5

03-14-2016-07:04:03 to 03-14-2016-08:04:03

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
66.249.75.215	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
220.231.195.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.194	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.139.91	147.237.72.166	Vietnam	aka.idf.il	ET SCAN NMAP -sS window 2048	1
42.116.139.91	147.237.72.166	Vietnam	aka.idf.il	ET SCAN NMAP -f -sS	1
37.26.149.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.37.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.35.64.142	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
42.116.139.91	147.237.72.166	Vietnam	aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-14-2016-07:04:03 to 03-14-2016-08:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	51
31.168.239.154	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
31.168.239.154	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	9
2.54.48.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
138.134.192.10	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.81.37.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.71.6.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
109.64.41.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.7.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.48.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.64.124.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.48.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.121.206.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.237.208	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.123	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.94.180.12	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.53.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
5.28.172.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.48.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.146.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	3
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.123	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.134.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.150.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.48.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
80.246.137.31	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
212.199.15.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.42.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.230.16.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.25.42	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.6.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.220	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.28.83	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.32	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.169.28	Israel	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
188.120.154.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
2.54.146.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.172.236.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

03-14-2016-07:04:03 to 03-14-2016-08:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.201.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.13.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.104.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 109.67.239.141	Block	1
2.54.146.135	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method SÓ[[#19]]vuÄ•-ŽsŠ°×çaE)[[#14]]Â¨Ø*)h8Q…©[[#20]]o„¡§S[[#26]]MDfLi ‡~I92[[#7]]¦K³#[[#23]]f_ú[[#15]]©Î–5Yºt1HÇ¦[[#11]]DìFÜpì•Œöµ[[#28]] æL4O¿déÀá•c[[#7]]9Ý~Ž¡ ÈïT°z)FàNqåŸ±¥å[[#1]]!ØÃ„Ž[[#22]]b1[[#31]]¿ ®[[#29]]®+Æ‹ÂhA¤œˆ·xt$ÿ[[#8]]æÍ[[#29]]ŒˆÙ_IÛÿ¼Eƒx[[#24]]Ë•Eó•… HoƒJã[[#7]]¦Ý[[#4]]ÒÚr¶ú…[[#11]]©]æ;4[?¤s3Í[[#31]]sE¬X¡å-o[[#15]]³Ãœ 0rMw-ëV*ÔzHµ¦vV[[#8]]ÀQ'f…xv˜˜QÓ2_É;~„æ}ŒË1¡hŽ6[[#31]][[#6]].-w [[#24]]2”[[#22]]˜ô¢/gâzuÅ¤ŽÐHäåç[[#29]]e[[#2]]ãùgG^!:{dSzV‡Œ[[#8]] [[#14]]ôìjgâ[[#25] Block	1
80.178.191.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 109.67.239.141	Block	1
65.55.210.104	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 109.67.239.141	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3058.jpg	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 37 Headers	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.67.239.141	Block	1
37.26.148.220	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL h[[#6]]g”["ɹû]#012i„[[ɲ#28[[]]#2ˆ‡]] c>ʌsᖷ9[[^|½ˆ¸¾ɲ#25l¸]]ʊ[[62#]]	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
80.246.136.93	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.67.239.141	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.67.239.141	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method SÓ[[#19]]vuÄ•-ŽsŠ°×çaE)[[#14]]Â¨Ø*)h8Q…©[[#20]]o„¡§S[[#26]]MDfLi ‡~I92[[#7]]¦K³#[[#23]]f_ú[[#15]]©Î–5Yºt1HÇ¦[[#11]]DìFÜpì•Œöµ[[#28]] æL4O¿déÀá•c[[#7]]9Ý~Ž¡ ÈïT°z)FàNqåŸ±¥å[[#1]]!ØÃ„Ž[[#22]]b1[[#31]]¿ ®[[#29]]®+Æ‹ÂhA¤œˆ·xt$ÿ[[#8]]æÍ[[#29]]ŒˆÙ_IÛÿ¼Eƒx[[#24]]Ë•Eó•… HoƒJã[[#7]]¦Ý[[#4]]ÒÚr¶ú…[[#11]]©]æ;4[?¤s3Í[[#31]]sE¬X¡å-o[[#15]]³Ãœ 0rMw-ëV*ÔzHµ¦vV[[#8]]ÀQ'f…xv˜˜QÓ2_É;~„æ}ŒË1¡hŽ6[[#31]][[#6]].-w [[#24]]2”[[#22]]˜ô¢/gâzuÅ¤ŽÐHäåç[[#29]]e[[#2]]ãùgG^!:{dSzV‡Œ[[#8]] [[#14]]ôìjgâ[[#25]]ç[[#27]][	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 109.67.239.141	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version ºèt{’•¼š¢»À9ÄåX·R[[#26]]Ø”{¿€uìab¥G„’ÔAÇŠBJÿa[[#1]] 1)¦õ‘·²Àü´[[#24]]œn[[#28]]¹C'†•^Ä÷üK[[#5]]³±‰½[[#4]]„Ì•Å˜òYuæ3ƒ •ºÉ[[#29]]—õ	Block	1
157.55.39.108	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
82.221.105.6	Iceland	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
66.249.69.169	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/templatecontrols/links/undefined	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at ²“v	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 109.67.239.141	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ²“v	Block	1
74.82.47.4	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 109.67.239.141	Block	1
46.249.151.48	Hungary	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/3347.jpg	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	NULL Character in Method Ö[[#15]]•.¹«Ô[ÖsÕIU×[[#2]]â¥$¹y3In…WÏqa^kŒR‹ˆÕºeÊØ[[#18]]`*ÍOj[[#7]]è[[#3]]ù\ )@ª[[#31]]Ò(ký[[#0]][[#14]][[#19]]«pŒŠââz[[#30]]Vm•¨Ázµ [[#18]][[#2]]7Iåƒ“ÀÕptn“äP•¤¬x@k¡•×ÝzˆÐwÌLƒ[[#23]]-÷¯e_[[#7]]&R ƒ&ÿœ‘s[[#7]]`[[#25]]F$pÚN‹×ëþ©ÌüþU,Ì•ŠÒ–±ÛÆ«»®ö&¶wŸšÅùclNb ×ƒå±7[[#31]][[#23]]è[[#25]]-I&á•×j·<£&žÔÿöÝð[[#5]] Êzÿè5QD:[[#26]] •¢KulÞÔãÚªó"ž˜â5aWi®ê¼{Ïµ°f¸¡‡•Z[[#29]]˜à,Ôtet[[#8]]	Block	1
2.54.48.191	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 109.67.239.141	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
131.253.25.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.53.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 109.67.239.141	Block	1
46.249.151.48	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	Malformed URL h[[#6]]g”["ɹû]#012i„[[ɲ#28[[]]#2>cˆ‡]]ʌsᖷ9ɱ¼¸ˆ½| ^[[#25]]¸l[[ʊ#26]]	Block	1
207.46.13.117	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1

03-14-2016-07:04:03 to 03-14-2016-08:04:03

03-14-2016-07:04:03 to 03-14-2016-08:04:03