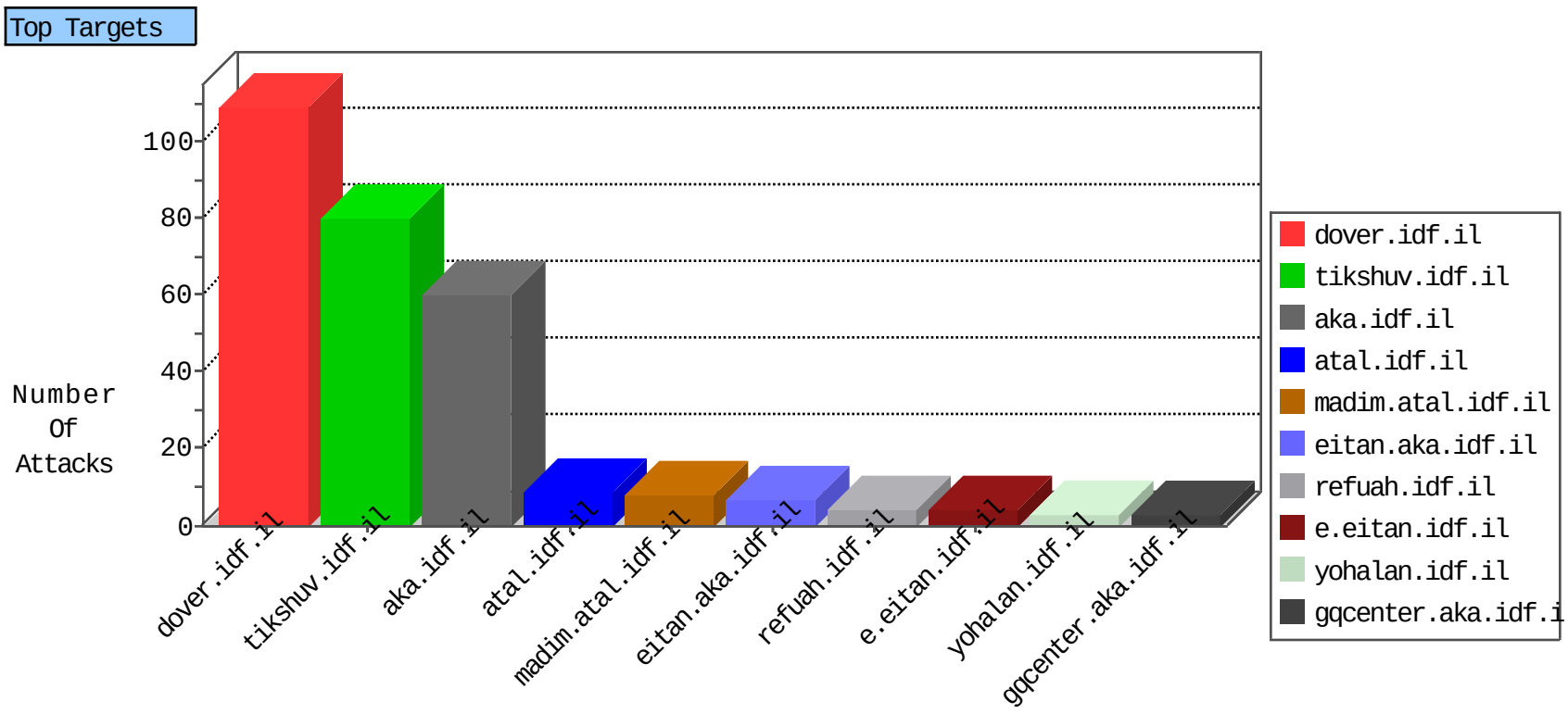
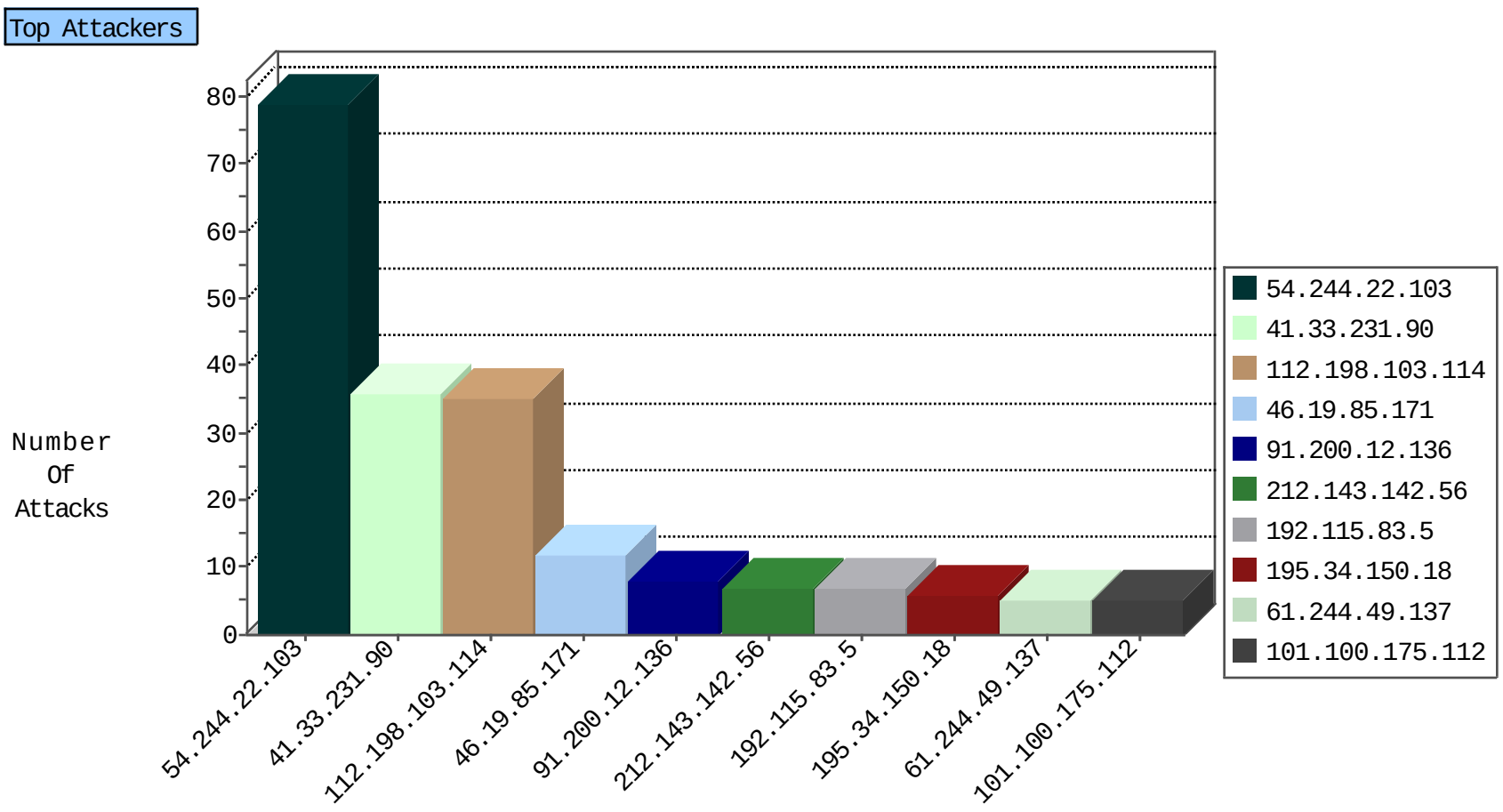
02-04-2016-03:04:09 to 02-04-2016-04:04:09

IDF Under Attack Daily Report





02-04-2016-03:04:09 to 02-04-2016-04:04:09

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
208.67.1.60	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
159.122.252.41	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

02-04-2016-03:04:09 to 02-04-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-04-2016-03:04:09 to 02-04-2016-04:04:09

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	3
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
101.100.175.112	147.237.76.199	Singapore	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
101.100.175.112	147.237.76.31	Singapore	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.238.230.133	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.76.196	Hong Kong	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.76.148	Hong Kong	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.137	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
101.100.175.112	147.237.77.216	Singapore	dover.idf.il	ET SCAN Potential SSH Scan	1
101.100.175.112	147.237.76.86	Singapore	navy.idf.il	ET SCAN Potential SSH Scan	1
101.100.175.112	147.237.0.15	Singapore	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.76.176	Hong Kong	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.137	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
185.106.92.137	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

02-04-2016-03:04:09 to 02-04-2016-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	76
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.171	Israel	147.237.77.216	dover.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	5
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
192.115.83.5	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
192.115.83.5	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
109.66.188.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.39.186.222	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
79.181.178.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
105.155.48.255	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
65.55.210.78	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
198.182.56.5	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.201.201.147	France	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.163	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
85.214.98.239	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
42.62.74.80	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
119.97.146.76	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
93.174.93.133	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.201.201.147	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.15.227	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.165	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
42.62.74.70	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.160	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
37.48.80.101	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.166	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
42.62.74.73	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.163.234.5	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.29.148.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
71.163.40.225	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.90.12.86	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.161	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

02-04-2016-03:04:09 to 02-04-2016-04:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.103.114	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 112.198.103.114	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.103.114	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 112.198.103.114	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 112.198.103.114	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.103.114	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.103.114	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method wÃ·:2Â•O[[#26]]Ã¶yo)g	Block	1
79.182.68.20	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$4 2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
191.232.136.77	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 112.198.103.114	Block	1
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$1 2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 112.198.103.114	Block	1
110.249.142.199	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/unauthorizedaccess.action	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Too Many Headers per Request - 63 Headers	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL k[[#12]]Æ'(f	Block	1
79.182.68.20	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
191.232.136.170	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-en	Block	1
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1086-en/eitan.aspx	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Unknown HTTP Request Method wÃ·:2Â•O[[#26]]Ã¶yo)g	Block	1
5.29.108.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
191.232.136.183	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
88.198.14.171	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	NULL Character in Header Name at ~Ã®Ãµ[[#7]]Â²FAÃ˜E3Ã·[[#5]]Âž =R7=_Â'0pÂ¾bk[[#11]]LÃ†J[[#16]]d[[#18]]Â£8lÂ¨Y[[#26]]/ÂŠÃŸ oÂ?Â?C[[#8]]Ã–bÂµyBÃ¿/Ã±Â¦Â¾y[[#29]]Ã›ÃœÃŸÃ› lÃ³@[[#27]]#Ã»Ã¬[[#30]]Â¸ ÃŒ[[#19]] Ã"Ã"ÃŽ[[#28]]BÂ¡Ã•Â¼Ã„Â¡Ã¢fÃ¸)[[#15]]Ã‡[[#20]][[#29]]Ã€8VÂ™ R[[#7]]8/Â™0Â [[#25]]o)Ã¸wGÂ¡[Ã?Â¹Â«%n (Â?[[#17]]Â?ÂŸ[[#12]]UÂŽÂ–,Â?=Â?b[[#18]]Â–Ã?58ÂŸÂ‰F4Ã´Ã¿Â–Â-Ã¼q[[#26]]Ã™Â„[[#27]]•Ã' K;Â?ÂŠÃ›?[[#18]]Ã³ÂŸÂ€Ã'ÂŸu]Ã–LÃ¢Â«EhÃ±Ã?ÂŽ\Â´Ã«Ã† Â·z_ÂºÃ¢Ã¬Ã-Â€[[#15]]Ã,Ã…Â»&Â?Â£ÃŠpÂ' Ã¤Ã?Â¥Ã¥[[#17]]Rq[[#14]]HQÃ¥Ã‡[[#0]]/92Ã–Â•	Block	1
66.249.69.90	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Illegal Parameter Encoding j.e[8l2tEjLR>S>2vSL;*$zzuM(&4WRz in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name ÃŸÂ„Ã"Â†[[#15]]ÂƒÃ´Â?#ÂŒ ÂŠÃ¸Ã´Ã·Âª[[#3]]Ã²Â¯Â"Ã?Q">"Ã Â¬Ã¬Ã¸Ã-jÂ¢Ã›Â‰Ã‡Â?"oV[[#22]]Ãƒ VÃ-Â¦][[#14]]Ã§ÃŒ[[#4]]Ã±Ã¥Ã•ÂŠQÃµÂƒÂ«Ã€Ã˜>Ã„ÂƒÂ›Ã—[[#17]][[#25]]`XÂºÃ'[[#19]]vEjmmQÃ?Ãœ Â´g'#Â?Ã²dpÃ"Ã¿[[#25]]b	Block	1
66.249.78.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
157.55.39.107	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 112.198.103.114	Block	1
8.37.70.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx&usg=alkjrhh_8otmlq723lo7rrg0kqg93wv-vq	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 5	Block	1
193.90.12.86	Norway	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
98.143.148.107	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/check	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	NULL Character in URL k[[#12]]Æ'(f	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 112.198.103.114	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
157.55.39.176	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19042-en/dover.aspx <a href=	Block	1
8.37.70.234	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhjxcetknzdsoafuks7qjluswatqqq	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Malformed URL k[[#12]]Æ'(f	Block	1
217.132.13.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	Block	1
110.249.142.199	China	147.237.0.17	m.my-kosher-kravi .idf.il	Unauthorized URL Access to 147.237.0.17/unauthorizedaccess.action	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":"	Block	1

02-04-2016-03:04:09 to 02-04-2016-04:04:09

02-04-2016-03:04:09 to 02-04-2016-04:04:09