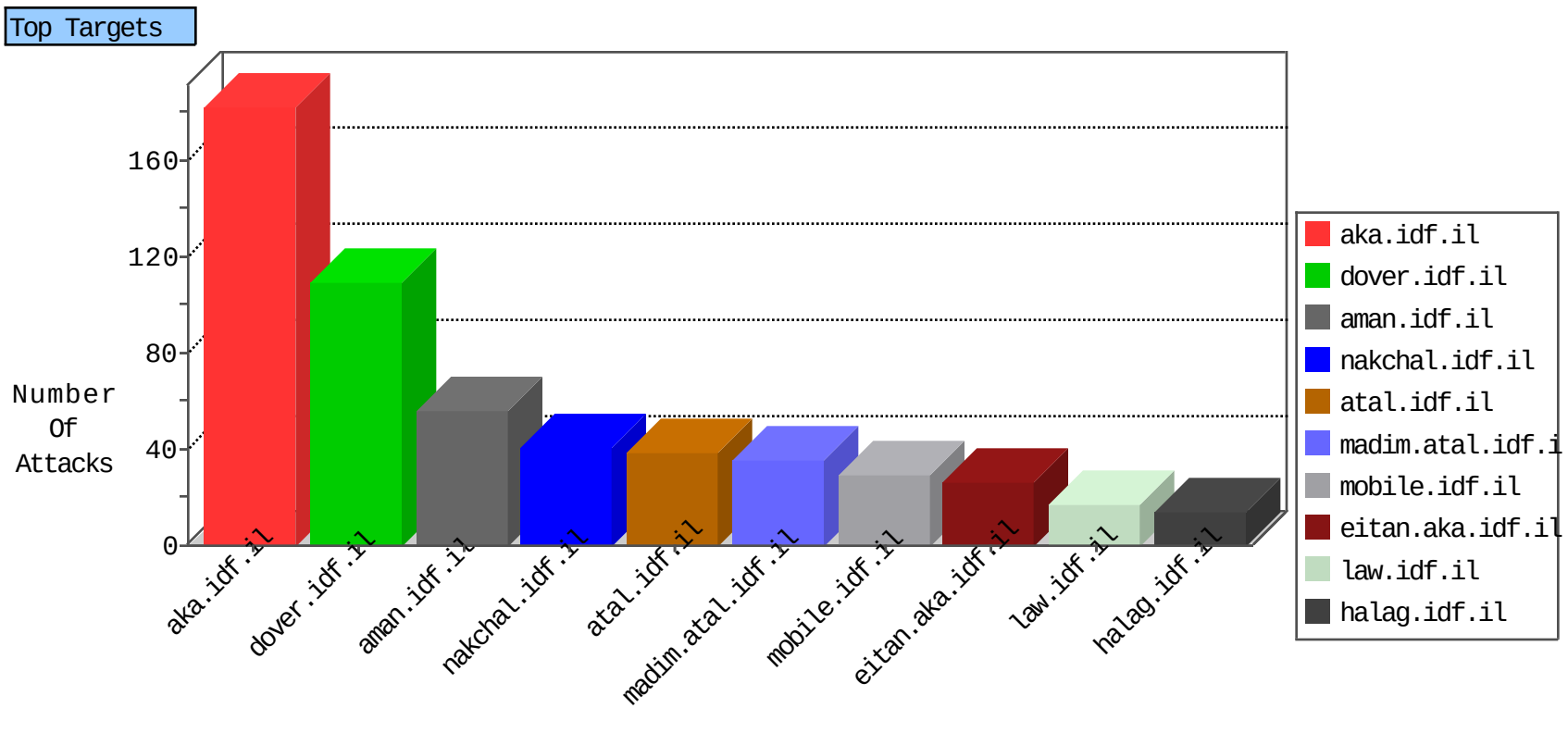
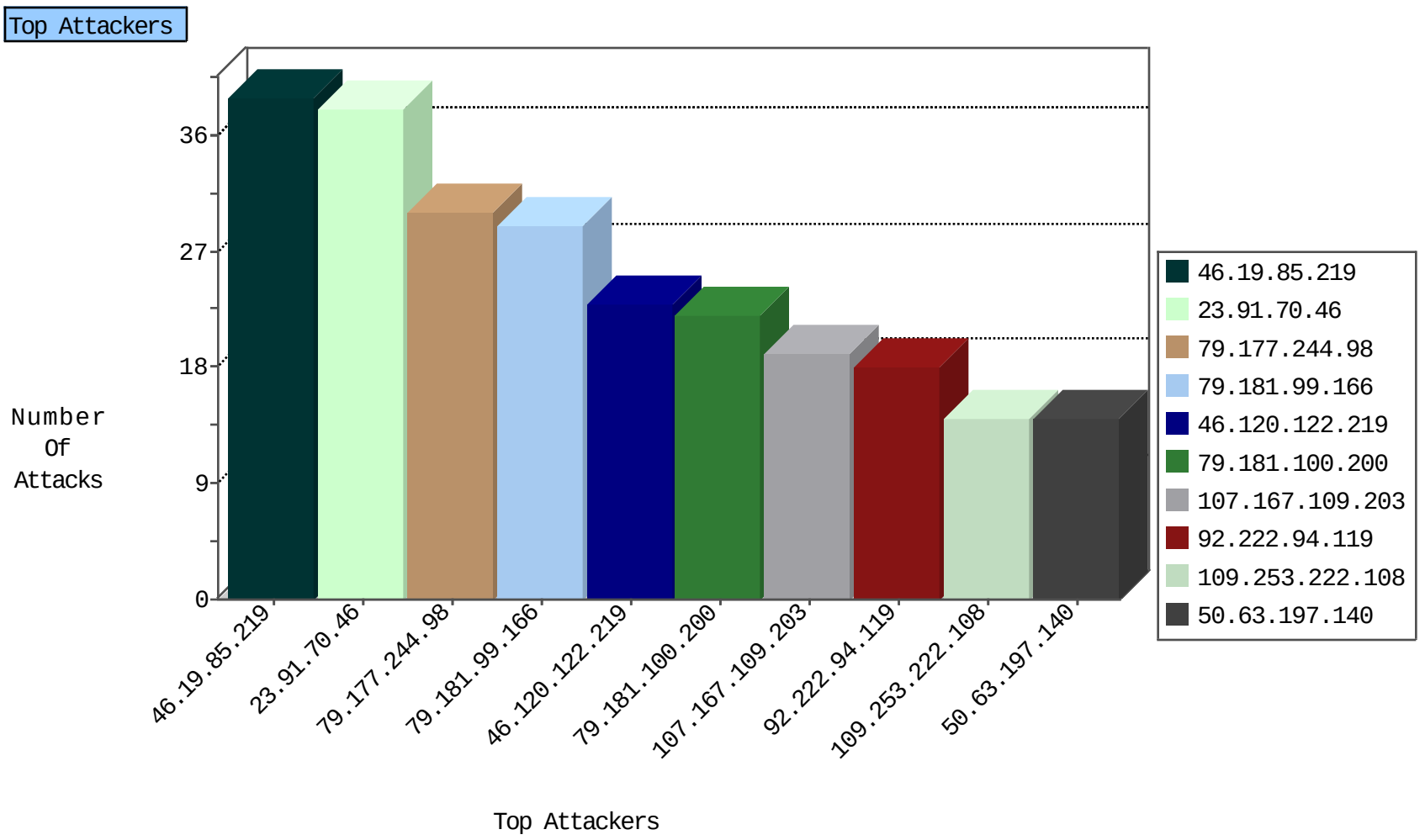
09-30-2016-16:04:08 to 09-30-2016-17:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-30-2016-16:04:08 to 09-30-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.85	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
2.53.164.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
71.6.216.43	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
123.249.0.134	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
217.146.166.26	Switzerland	147.237.8.24	e.lifestyle.idf.	L4 Source or Dest Port Zero	drop	1

09-30-2016-16:04:08 to 09-30-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.222.94.119	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	18
50.63.197.140	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.46	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.46	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.46	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
108.59.8.80	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
177.12.161.72	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-30-2016-16:04:08 to 09-30-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.181.100.200	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	22
23.91.70.46	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	12
50.63.197.140	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
63.221.141.195	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
146.200.148.0	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
115.239.251.250	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
115.239.251.250	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.187.129.107	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.175.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.85	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
115.239.251.250	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
115.239.251.250	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
115.239.251.250	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.138.119.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-30-2016-16:04:08 to 09-30-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.244.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.219	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
107.167.109.203	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
46.19.85.219	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
109.253.222.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
77.139.6.153	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
77.138.47.64	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
79.176.106.18	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.116.57.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.210.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
46.19.86.248	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.111	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
176.13.1.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.6.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
176.13.15.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.130.234.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
88.202.218.240	United Kingdom	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.2.161	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.207.137	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
46.19.86.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.207.137	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.209.50	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.199.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.108	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.208	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.176.76.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.100.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.116	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.209.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.209.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.64.25.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
141.226.218.116	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.8.204.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.182.141.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.110.55.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
199.30.24.127	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.55.168.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
138.68.73.252	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.209.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2

09-30-2016-16:04:08 to 09-30-2016-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	10
77.125.12.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
5.29.61.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.125.100.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
130.125.70.159	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/main.htm	Block	3
88.202.218.240	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
79.177.134.115	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.177.134.115	Block	2
2.53.132.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.34.240.227	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	2
185.120.124.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.181.5.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
183.89.25.207	Thailand	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
77.138.5.34	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name ì<[[#15]]yg¿[[#25]]<oÜz[[#12]]mŠG½[[#23]]•¶4IŠ¾[[#18]]Í¥•O˜"[[#30]]-Õ·[[#29]]ihx*ƒ…Â•ßÔ¡Z%Új·í [[#22]]ŽFämvt•™^[[#3]]òë*q°±hÁÃ•§€qé[[#22]]}¼2 ″"ÄG¤-ò‘"8	Block	1
109.253.207.137	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 7	Block	1
183.89.37.234	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
88.202.218.240	United Kingdom	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
77.138.19.115	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
192.243.55.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	1
66.249.64.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.185	Block	1
125.77.28.26	China	147.237.76.39	mobile.meitav.idf.il	Unauthorized Method HEAD for 147.237.76.39/	Block	1
79.178.194.157	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type text/ping	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Malformed URL 0[[#8]]ת³¨jj‹Ð„•–yƳ′eת²Ʊ~ƒ˜¼§	Block	1
185.27.106.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/cgi-bin/shitur/bookpage100598/iturfindpageexact.pl	Block	1
77.139.32.242	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method žHèñgQ}P£+£′Ñg·4‹rë{[[#25]]æ}[•j–=åéÄ¸#012′óá[[#3]]*n=â³ÖÛöñ[`6†Å¿•É.ESßà[[#25]]Ôþb:[[#2]]¶bÑm½¤}\çü9-è{•Ê²[[#19]]l¢[[#30]]Œ•i…;èt3w§ÌÒÁ	Block	1
66.249.64.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
79.180.210.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at [[#31]].[[#25]][[#15]]§¦¾•[[#18]]ÞÓ+?ëŽ,ë6>•vY“-•Þ 2′[[#14]]§[[#23]]N[[#22]][[#25]]Qò[[#6]]˜[[#15]]Óé[[#25]]»bÇCeIî[[#8]]7µ»<2kßÃÑÀSÂ[[#15]]UÀ‡ÆÛì-JÈ-PIŸ•ÊÂrÉ4•*-²ï–Žx°¬[[#0]]¢<é›»[[#3]]²¤o¡b"9*2a•[[#1]]HpÚŠ?[[#15]]œbiæ3/Ž¯Ú,{iŸ7Ž2²?_Ÿ[[#5]]@kµ¾•ÞÞh–”žï4jì¹‡·MA›¿pŠz$i[[#18]]pü_ðé#011r¼0´ð×˜7åìÚ•[[#3]][[#21]],Ê‹d³mFSoÎ`d¨?,SwpŒÝ)[[#15]]-—ÞÝžÕdå•Á••[[#31]]©^Dg Ú—™%ÍÚ′[[#4]]×Í â[[#27]]Çç[[#22]]çÏ7ÙÖÑš;<nG•¼[[#29]][[#26]]¥À[[#18]]!,Ê³[[#2]]È©¯àñ0Û·™¿i/¯eYÑ÷ó94v¨à¤v zÖ#x[[#11]]′[	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
46.120.165.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
93.172.155.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.138.198	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL 0[[#8]]ת³¨jj‹Ð„•–yƳ′eת²Ʊ~ƒ˜¼§	Block	1
213.8.204.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69849.pdf	Block	1
178.32.153.219	France	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Unknown HTTP Request Method žHèñgQ}P£+£′Ñg·4‹rë{[[#25]]æ}[•j–=åéÄ¸#012′óá[[#3]]*n=â³ÖÛöñ[`6†Å¿•É.ESßà[[#25]]Ôþb:[[#2]]¶bÑm½¤}\çü9-è{•Ê²[[#19]]l¢[[#30]]Œ•i…;èt3w§ÌÒÁ	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
77.127.241.20	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.67.51.253	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1

09-30-2016-16:04:08 to 09-30-2016-17:04:08