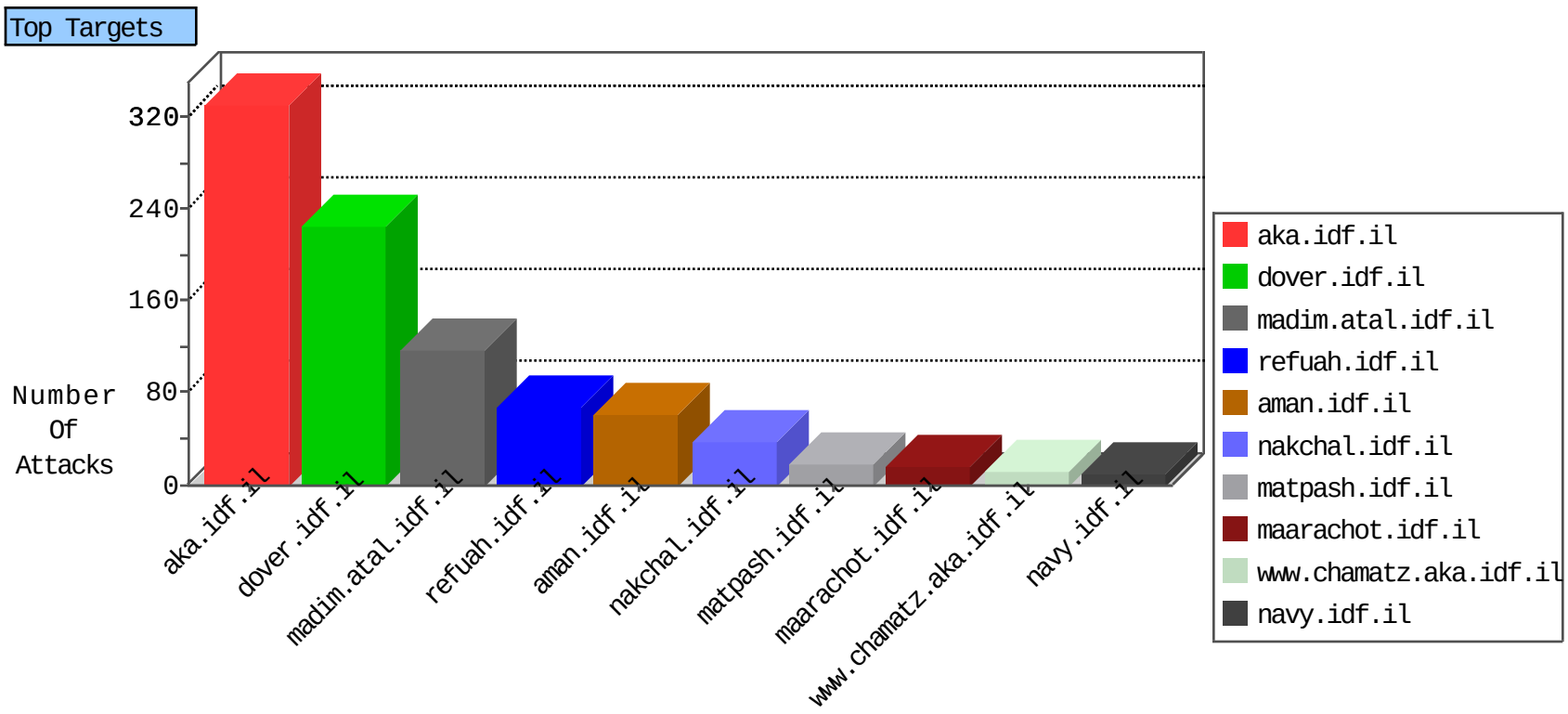
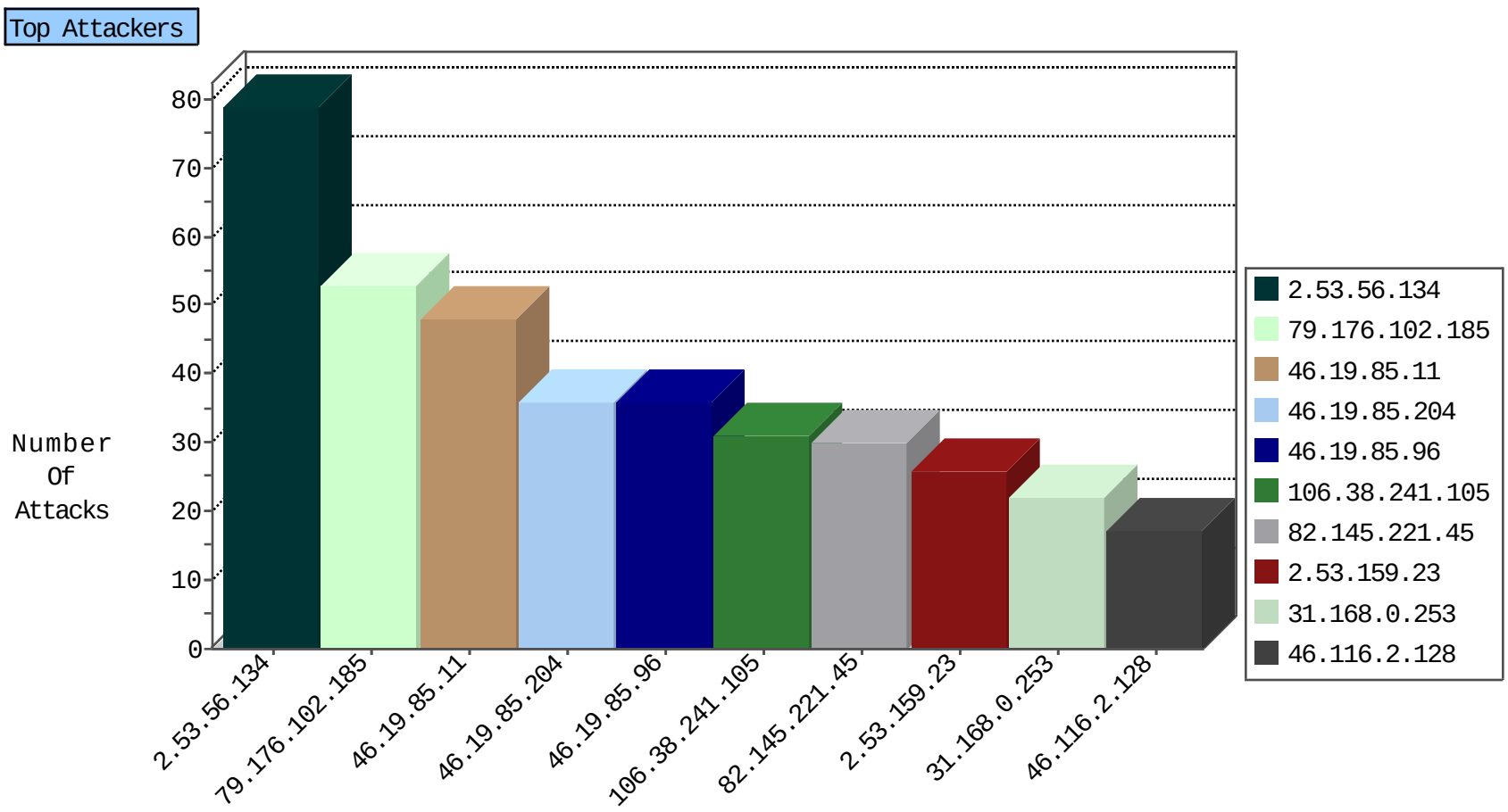
09-13-2016-21:04:06 to 09-13-2016-22:04:06

IDF Under Attack Daily Report



Top Target



Top Attackers

09-13-2016-21:04:06 to 09-13-2016-22:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.28.22	Israel	147.237.72.166	aka.idf.il	Black List	drop	6
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
216.26.141.6	United States	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.26.141.7	United States	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.41	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-21:04:06 to 09-13-2016-22:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.i	C1000071: HTTP: User Agent Sogou+web+spider	Permit	29
123.126.68.131	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
212.252.57.54	Turkey	147.237.77.216	dover.idf.i	C1000016: HTTP: administrator in URI	Permit	1
212.252.57.54	Turkey	147.237.77.216	dover.idf.i	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

09-13-2016-21:04:06 to 09-13-2016-22:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
2.55.9.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.53.227	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	1
50.116.123.135	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.138.146	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.166.138.146	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.76.34	Moldova, Republic of	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.138.146	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
104.167.6.84	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 2048	1
41.60.209.91	147.237.77.179	Zambia	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.72.156	Ukraine	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
77.138.52.97	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.166.138.146	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
46.166.138.146	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.76.198	Moldova, Republic of	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.138.146	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.153.197.30	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
91.201.236.158	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -f -sS	1

09-13-2016-21:04:06 to 09-13-2016-22:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.221.45	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.11	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
31.168.0.253	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
5.102.197.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
188.161.61.183	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.11	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
113.210.54.37	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
87.69.221.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.116.2.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
77.56.193.12	Switzerland	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
173.178.137.220	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
95.224.118.204	Italy	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
2.53.134.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.225.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
5.102.195.103	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.244.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
24.222.4.86	Canada	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
87.69.79.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.116.2.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.15.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
95.224.118.204	Italy	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
124.125.240.86	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.55.29.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
5.29.213.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
95.224.118.204	Italy	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.3.147.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
115.250.20.178	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.18.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.25	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.116.2.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.149.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.66.143.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
95.86.114.40	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.188.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.56.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
2.53.159.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
89.138.185.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	13
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	5
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	5
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	5
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.176.102.185	Block	4
2.53.20.38	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	4
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.176.102.185	Block	4
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.176.102.185	Block	4
5.102.195.103	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.176.102.185	Block	3
109.65.176.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.70.15.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.170	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	2
24.120.53.171	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2016/lobby.aspx	Block	2
77.139.26.222	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.176.102.185	Block	2
46.121.98.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.176.102.185	Block	2
77.138.211.99	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	2
2.55.36.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
200.111.107.58	Chile	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/index.php	Block	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name •][[#20]]SDwV~[[#28]]€•¢f•{.Êû0[[#30]]ð=dXÔ_â©jªÅ[[#16]]]ô«¸J[[#24]]Cf ÖŒÒjªÚ`•mºr@Lü)^´-¡Ý„&ú[[#8]]H‘*ÿ9Ú[[#0]]¸öÄæ¿L‹zï7ùÖŽg[[#6]]ùê· ÀòI2RD[[#16]]Ûx•Jc}.·\¾[[#18]][[#15]]uW!þ[[#30]]!$[[#31]] ŠÜ…•Y‰6rC£‰•Ñnâ[[#31]]ŠòŽuÞ[[#17]]V"4àÖ8ð¸i[[#29]][[#17]]cGì[[#29]] ÝÎ®[[#23]]LMh	Block	1
77.139.167.27	France	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
87.69.78.86	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.176.102.185	Block	1
77.138.14.251	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version T[[#14]]t±šóVîþ>~JàßT[[#31]]ñEÞÆ,v‰¾ï*Y0ÈÑ3æöµ½¶ÀØà#012![[#27]]yâ» [[#31]]ÕgXúŠ•[[#26]]e·Ì•-,¼_1gsž“ù[[#2]]ú`Œ÷ª[[#17]]âs¼»4Ï1E]ä[[#17]] ″F]fQ³‹…[[#2]][[#29]]î‹Oþ2J*€ì¡¨…G@Ñ•~öæê°´•Xø}¥Ñ2ÓE3`´ÇH.[[#5]]åð ÚÞòµšXLÝ[[#12]]ÄÛ,[•:rß[[#0]]ó±ŸÅ[[#22]][[#4]][[#23]]uÁw•#ý¯•ü#Moè[[#19]]tØc¤•Jê%[[#3]]3÷G’•[[#5]]ž78…Å[[#5]]¾t˜~c?[[#19]]H	Block	1
31.168.0.253	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.9.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
109.67.222.125	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	NULL Character in URL f°[[#6]]b[[#1]][[#0]]″•¥ßÝ[[פ#1[[ֽ§ׂצֹ]]#30©:]]2™ï¿šqr qs\[[#11]];¾ם1[[#31d8e]]ט^ֽ‰o]]13#[[Ú]]1#[[ֶ]]3#[[ržk¿בx	Block	1
77.139.3.39	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.3.39	Block	1
46.19.86.212	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method l/1127-he/IDFG.aspx in URL	Block	1
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
77.139.167.27	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 79.176.102.185	Block	1
77.138.25.73	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
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding e>[[#16]]Ý°s_$םq•{¬oü×[[’§ ;#14'_¡ f]]ך’Þi• >jqœ§Ÿ~bÊŠ·ֽzֽ ¡jƒhטn±"טŒ›¶Û³b[[#22[[ֽ[]]#7kk˙zn ֽk<†]]לֽ;	Block	1
176.13.250.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.139.17.78	France	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
79.176.102.185	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ŒÒjhpGtùÃGè[[#1]][[#26]]ó••¿<·[[#16]]2oÍu	Block	1
213.151.49.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in aka.idf.il/main/sachar/payslips.aspx	None	1
77.139.201.3	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1