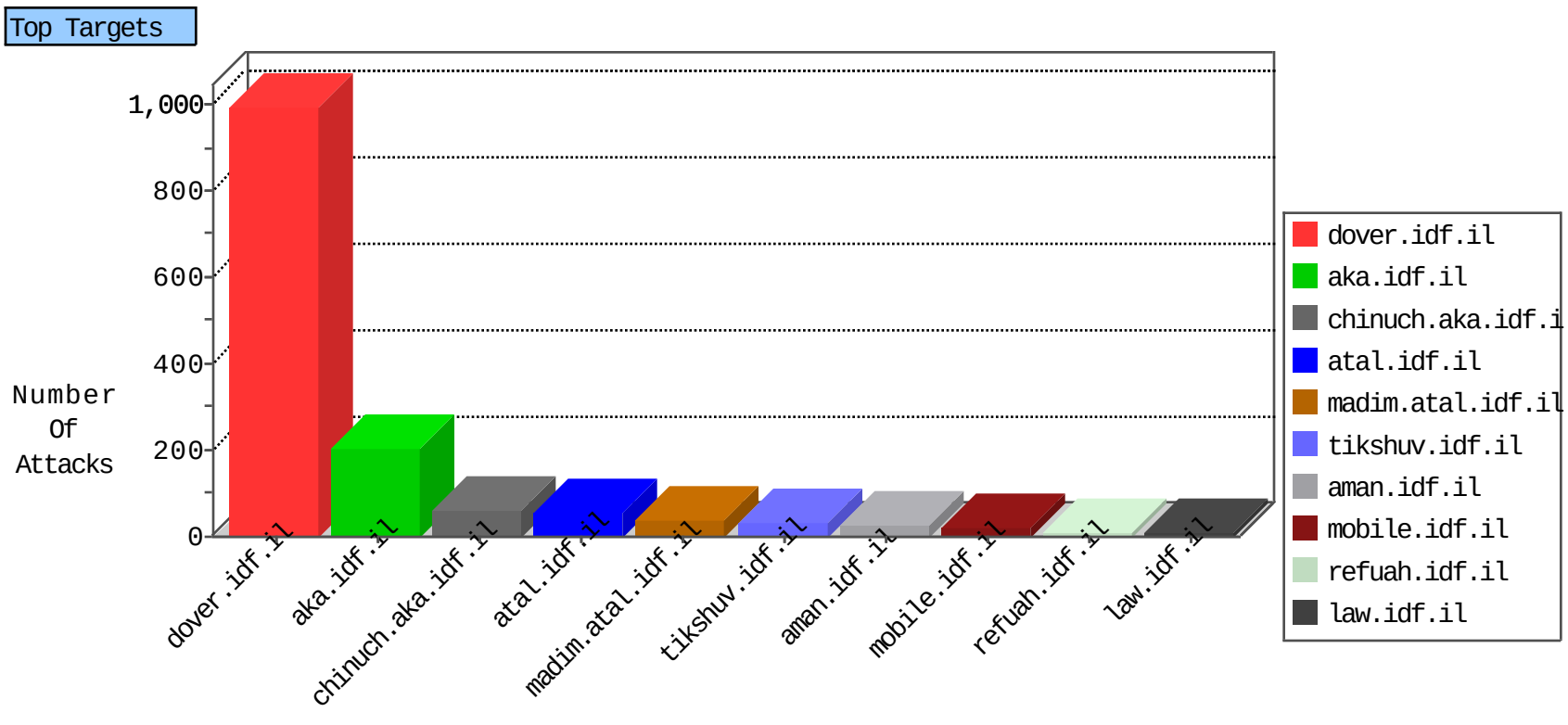
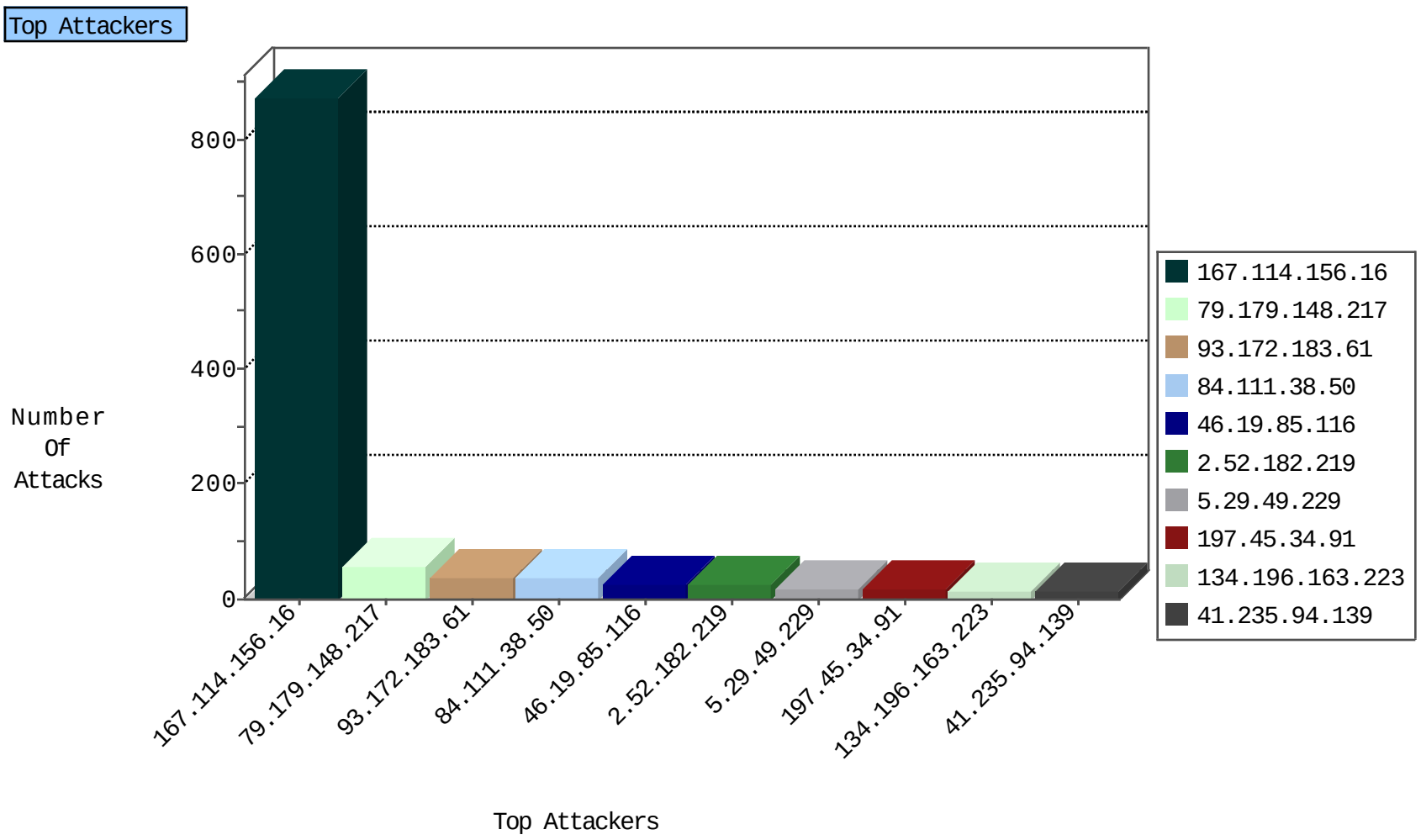
03-11-2016-15:04:04 to 03-11-2016-16:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-11-2016-15:04:04 to 03-11-2016-16:04:04

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	3139
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
89.248.167.162	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1

03-11-2016-15:04:04 to 03-11-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.100.76	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
109.65.11.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.67.144.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
10.0.0.3		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
77.125.107.136	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.134.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
173.208.136.170	United States	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
188.165.15.223	France	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
191.236.119.223	United States	147.237.0.17	m.my-kosher-kravi.idf.il	0947: HTTP: test-cgi Access	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
191.236.119.223	United States	147.237.0.19	madim.atal.idf.il	0947: HTTP: test-cgi Access	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
191.236.119.223	United States	147.237.0.34	tikshuv.idf.il	0947: HTTP: test-cgi Access	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-11-2016-15:04:04 to 03-11-2016-16:04:04

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
109.253.132.158	147.237.76.42	Israel	refuah.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
88.249.106.23	147.237.77.226	Turkey	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
194.0.129.99	147.237.0.34	Romania	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
189.218.48.7	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.189.26.18	147.237.77.226	Austria	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.57	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1

03-11-2016-15:04:04 to 03-11-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.148.217	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
93.172.183.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
134.196.163.223	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
79.183.16.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.182.219	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
5.29.49.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
197.45.34.91	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.181.37.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.177.219.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.45.34.91	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.182.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.182.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.182.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
185.3.146.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.80.182	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.125.50	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
41.235.94.139	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.238.243.41	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
41.234.76.28	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.69.146	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
41.234.76.28	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
89.138.5.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.190.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.29.49.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.238.243.41	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.250.147.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.6.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.56.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.17.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.56.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.172.165.189	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
109.65.145.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.144.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.24.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.227.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.144.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.186.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.235.94.139	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.149.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.33	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.49.229	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.64.149.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.142	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3

03-11-2016-15:04:04 to 03-11-2016-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
2.54.53.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 84.111.38.50	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 84.111.38.50	Block	2
89.138.104.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 84.111.38.50	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 84.111.38.50	Block	2
149.78.169.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 84.111.38.50	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 84.111.38.50	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 84.111.38.50	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 84.111.38.50	Block	2
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 84.111.38.50	Block	2
103.237.74.198	Hong Kong	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
79.177.219.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.64.26.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.153.113.13	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ŠCýÎHóp/[[#2]] in URL ‡[[#8]]^j[[#0]]f	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
5.29.49.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 84.111.38.50	Block	1
109.253.205.138	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ŠCýÎHóp/[[#2]]	Block	1
79.180.135.62	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
87.97.9.51	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at €ðÒ§+6ÀïQ/Dú¾07ðÜ„¹#012–¢Ø§*[[#31]]ešËŽ*NB¢+=Xi4ñW[[#21]][[#8]]ZÙƒŸÀX5\ˆ•êù[[[#6]]]_ª¹ÃÂ‹i[[#30]]èš!Díw±[[#28]]©Ü%Xrì‰¿[[#18]]k¡øAgÔbêª[[#6]]Å„ØA2i±sâ£¡²@Ã[[#29]]\f,Þn[[#24]]ù#k¸ç¦Ã[[#3]]ÝC³m[[#30]]«xËUÞf6[[#11]]O“[•$±!‰[[#28]]ÐZDt[[#20]]•³•N])›Ï!‹ì•»[[#28]]#011z4¹þä~Lä“U¢Ê$BC±ÏÆ[[#4]]){«™#012 ,6µüe[[#8]]xPhu[[#2]]£ô³`²[[#18]]•%[[#1]]¿g[[#25]]ªÕÊIV³nóœÙ€S`O[[#29]]x[[#2]].1,;mkXhù¦Vûò]½	Block	1
46.60.93.160	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.95	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
93.172.183.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
68.180.228.102	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.142.64.26	Israel	147.237.76.39	mobile.meitav.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version •ì‡&(DZ ‡Ü§•×o²[[#27]]*Cêþ[[#2]])M.ÜŒÓÙŽ-Wô>ƒ'VWŠËƒ}ÖŸø¹&GÞÛEj7<• !3²Çr[[#19]][[#3]]¾T6[[#7]]hþmïF]÷øý¨[[#16]]èŠÜ¦[[#17]]°;IIÿ¾äÃ¸^[[#24]][[#20]]ixl[[#5]]Êm5[[#7]]Z¯6H\5$ü\FgcÐ[[#31]][[#5]]1Fà©6[[#7]]þWY ••üÙ[[#30]]ˆeüŽ¿F»5ßÖS/¨[[#7]] ò+W[[#0]]—uz•‹yÆ0›ÜË;,-#×[[#21]]°[[#2]]`-=[[#11]]ÎÞg^w“”Ee[[#16]]•ò,d[[[#19]]"}¥Â«Aê[[#18]]®¸çÔÝ“î;ëîÔÌFK”¦«!Œ‡¢ø•ßx¹HaÉ™Ð±Æ¥ÊýŠ†Éó˜ô[[#29]][[#26]].„Ë¯N[[#26]]‡µb»JÖÞ[[#17]]—]¯¼¶Xoäa ÑÈ@vOÕ[[#22]]t÷P;A•¦Ë+÷àÑÃ¾v•@¬‹Î[[#5]]Zf¸Z81¡UÿúBPL´ÓLÅ“nGÅF¶FVç[[#29]]au	Block	1
79.182.246.241	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
87.109.169.43	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	NULL Character in Method £ÅÖy™—vô4¹qð[[#22]]D[[#2]][[#8]]†cR:n[[#0]]Á% Mj4	Block	1
46.117.80.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
213.151.36.128	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
94.230.93.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.82.47.4	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
84.111.38.50	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
37.142.68.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar.aspx	Block	1
84.111.38.50	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 22	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
79.183.52.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

03-11-2016-15:04:04 to 03-11-2016-16:04:04