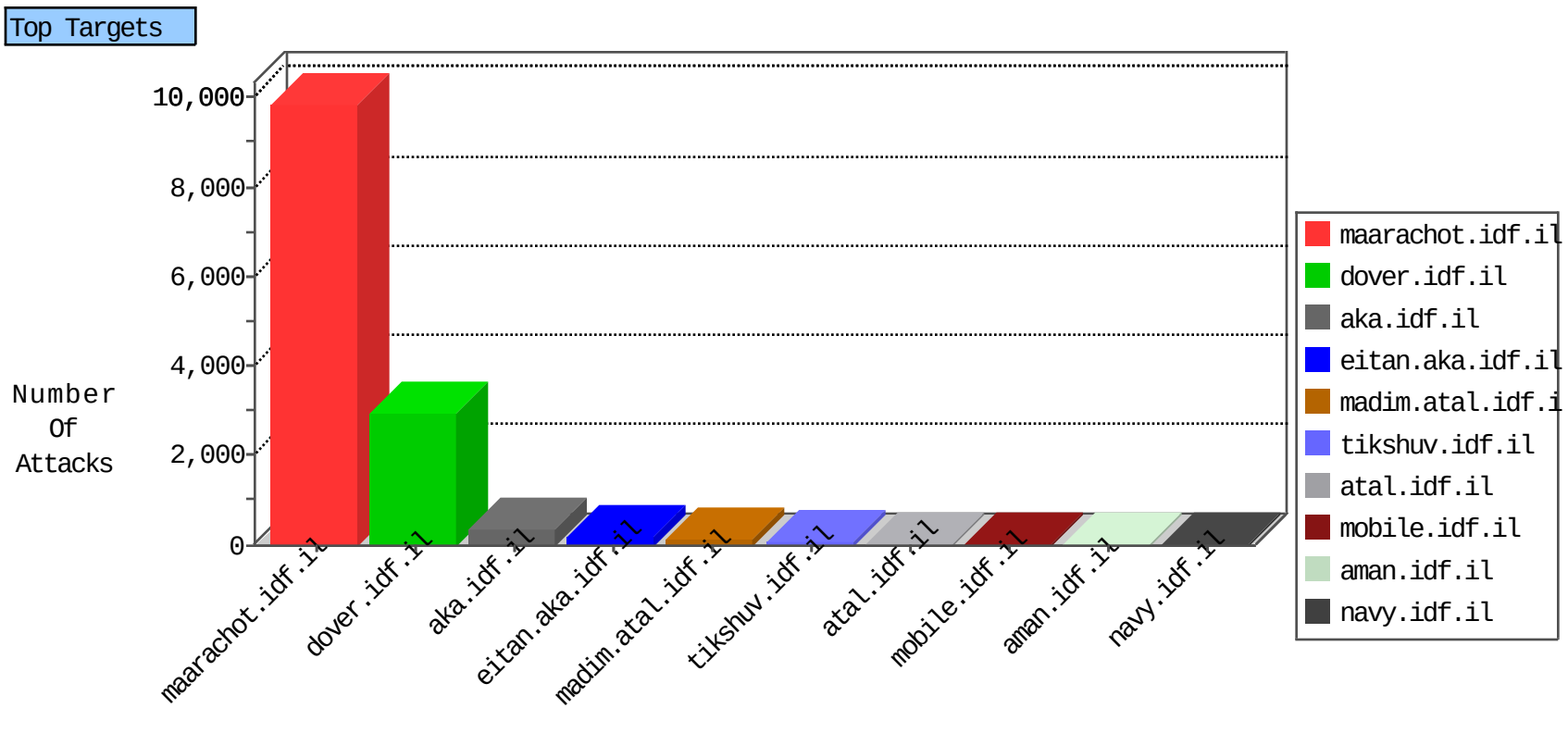
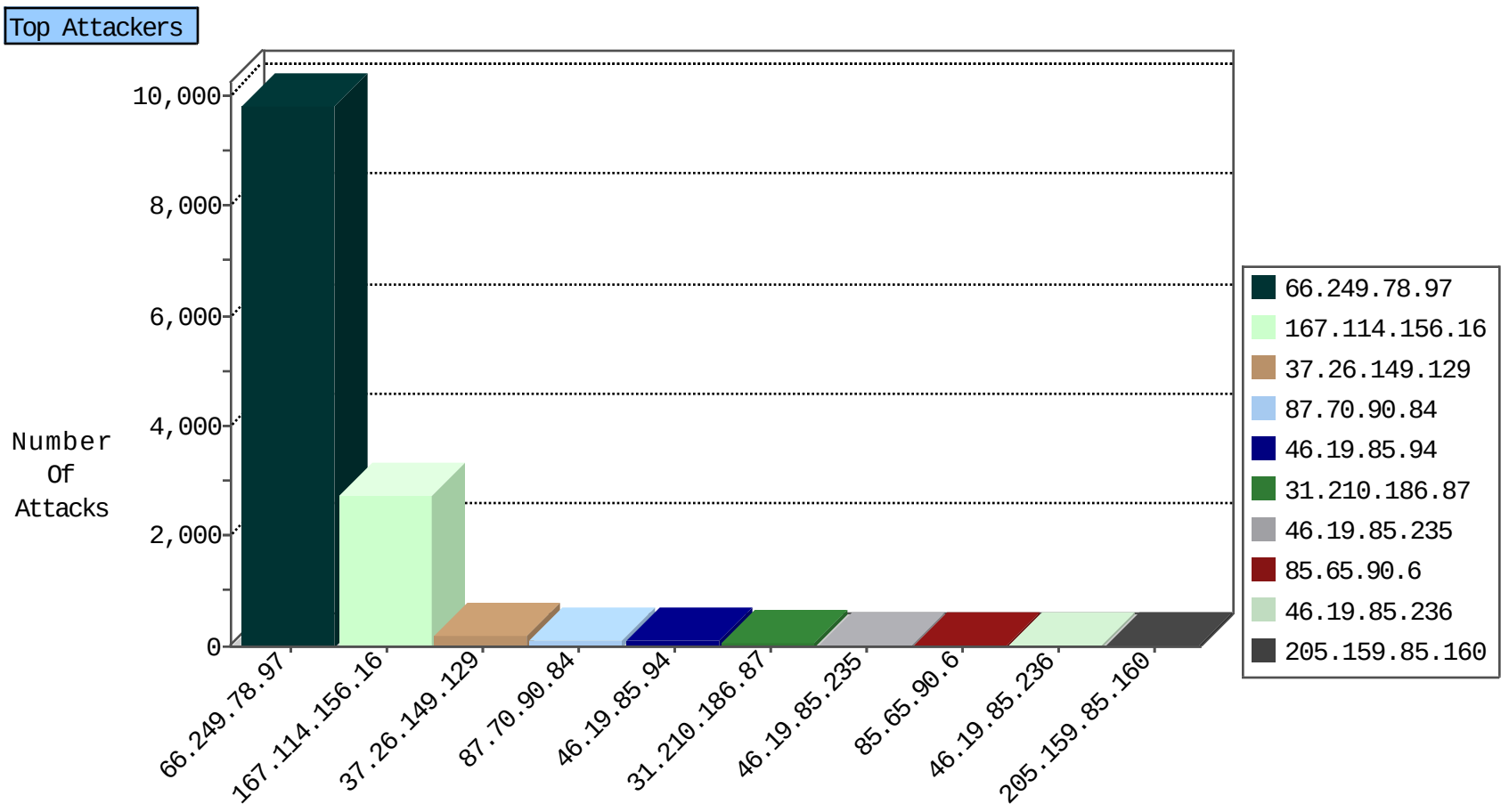
03-15-2016-22:04:06 to 03-15-2016-23:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-15-2016-22:04:06 to 03-15-2016-23:04:06

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	3622
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
180.97.31.70	China	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid L4 Header Length	drop	1

03-15-2016-22:04:06 to 03-15-2016-23:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.88.145.165	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
176.228.160.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.52.29.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.29.21.152	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.88.80.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.129.88	United Kingdom	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Block	2
95.86.101.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-15-2016-22:04:06 to 03-15-2016-23:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	9833
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.8.120.111	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
190.196.178.78	147.237.76.86	Chile	navy.idf.il	ET SCAN NMAP -f -sS	1
95.173.184.200	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
37.139.27.231	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.178.78	147.237.76.86	Chile	navy.idf.il	ET SCAN NMAP -sS window 2048	1
185.85.190.98	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
74.208.238.221	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
60.217.72.16	147.237.0.33	China	idf.il	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	1
222.186.56.18	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.196.178.78	147.237.76.86	Chile	navy.idf.il	ET SCAN NMAP -sS window 4096	1

03-15-2016-22:04:06 to 03-15-2016-23:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.129	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	171
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
31.210.186.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
85.65.90.6	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
205.159.85.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
31.210.186.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
2.54.158.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
82.166.181.40	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.108.239.8	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
178.39.218.11	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.171	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.182.149.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
80.178.159.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	8
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	7
84.108.239.8	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.206.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.84.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.159.239	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.4.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.15	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.122.213	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.7.51	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.91	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.147.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.73.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.170.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.38.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
77.126.148.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
24.164.130.147	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.44.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
87.71.242.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
40.77.167.58	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
141.0.15.20	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.116.167.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.177.139.207	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.52.162.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.9.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.74.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-15-2016-22:04:06 to 03-15-2016-23:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
2.54.156.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 87.70.90.84	Block	5
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 87.70.90.84	Block	5
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 87.70.90.84	Block	5
77.126.41.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
176.13.0.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 87.70.90.84	Block	4
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 87.70.90.84	Block	3
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 87.70.90.84	Block	3
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 87.70.90.84	Block	3
176.100.124.130	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.100.124.130	Block	3
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 87.70.90.84	Block	2
188.162.39.104	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	2
188.162.39.104	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in www.tikshuv.idf.il/site/general.aspx	Block	2
89.138.56.66	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 87.70.90.84	Block	2
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.70.90.84	Block	2
79.179.127.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation searchText in www.idf.il/1518-en/dover.aspx	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding [[#14]]%gÝÛ[½l[[#30]]©′&y˛9ר•Ðš¦'a8%Т [[#25]]•;¾r˛¾Û˜%[[#23]][[#22]]g[[#15]][[#2]][[ץ#15£$]]b¢[[#29]]k† >šfח•w©x>רh]	Block	1
46.116.107.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	1
176.100.124.130	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1395-en/dover.aspx'	Block	1
109.64.179.80	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at [[#18]]³¦gEÃ¨ÒÄ¥[[#26]]p"Õ[[#15]]z[[#18]]†,Jô‡Ùƒ4[;•pìá“[[#7]]ØÒ±µ Q¬L[[#12]][[#16]]›y[[#18]]?ìŽÀ[[#30]]êƒvh[[#16]]ˆ•™•#Ä[[#21]]î[[#3]] Íáƒ”˛ž[[#23]]´„ñüe\2»C…cž‘V,¤bƒ±‹Nå‹••@ƒ••02Ä[[#7]]Vn[[#5]]Á Ý±n4Eª[[#4]]s2ñ—¡pTT%Ç$²vl[[#22]]Ó£m«[[#15]]-)®åe[[#30]]CôÌÓP…m[[#12]]ŒÔ?W`ÙÓAÖƒ[[#24]]OTð[[#4]]•—É[[#22]]$6aÚH#3'mø{9èB´ü• 9ý [[#16]]ýÚËkß°	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/109236.pdf	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name R[[,כרר#0ו˛†-]]r±[[#30]]ץ [[#0]]vŽO°″aוB[[#3]]ב¾û-•²C[[#27]]€t[[נ'›ם#24ח]]V:« in …:ƒ [[#23]]fi#012rŒ[[#6]]ƒ§a{¶Ž1כ÷n ″]פt„-q!Ý‹	Block	1
40.77.167.16	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on tikshuv.idf.il/site/general.aspx parameter catId	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.193	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ¿ß9ó	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
178.248.90.71	Italy	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 2	Block	1
65.55.210.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.144.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
66.249.79.176	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	NULL Character in Method %hGÒÔÙþ[[#12]]E¿Ç¶€gµB«[[#2]]¸yp[[#27]]ÀsŠ5VúõšË›ï^=öQx(ï¿ŠNåU V[[#4]][[#19]]÷œ-+ièrÑ`[^T-B:ÇÞ•Á²[[#1]]/ÆÏ}Y][[#27]]Êœ0Dî[[#0]]Øj	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/106567.pdf	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String R[[,כרר#0ו˛†-]]r±[[#30]]ץ [[#0]]vŽO°″aוB[[#3]]ב¾û-•²C[[#27]]€t[[נ'›ם#24ח]]V:« on …:ƒ [[#23]]fi#012rŒ[[#6]]ƒ§a{¶Ž1כ÷n ″]פt„-q!Ý‹	Block	1
40.77.167.104	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
173.195.13.228	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.126.41.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3338.jpg	Block	1
212.76.112.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1

03-15-2016-22:04:06 to 03-15-2016-23:04:06