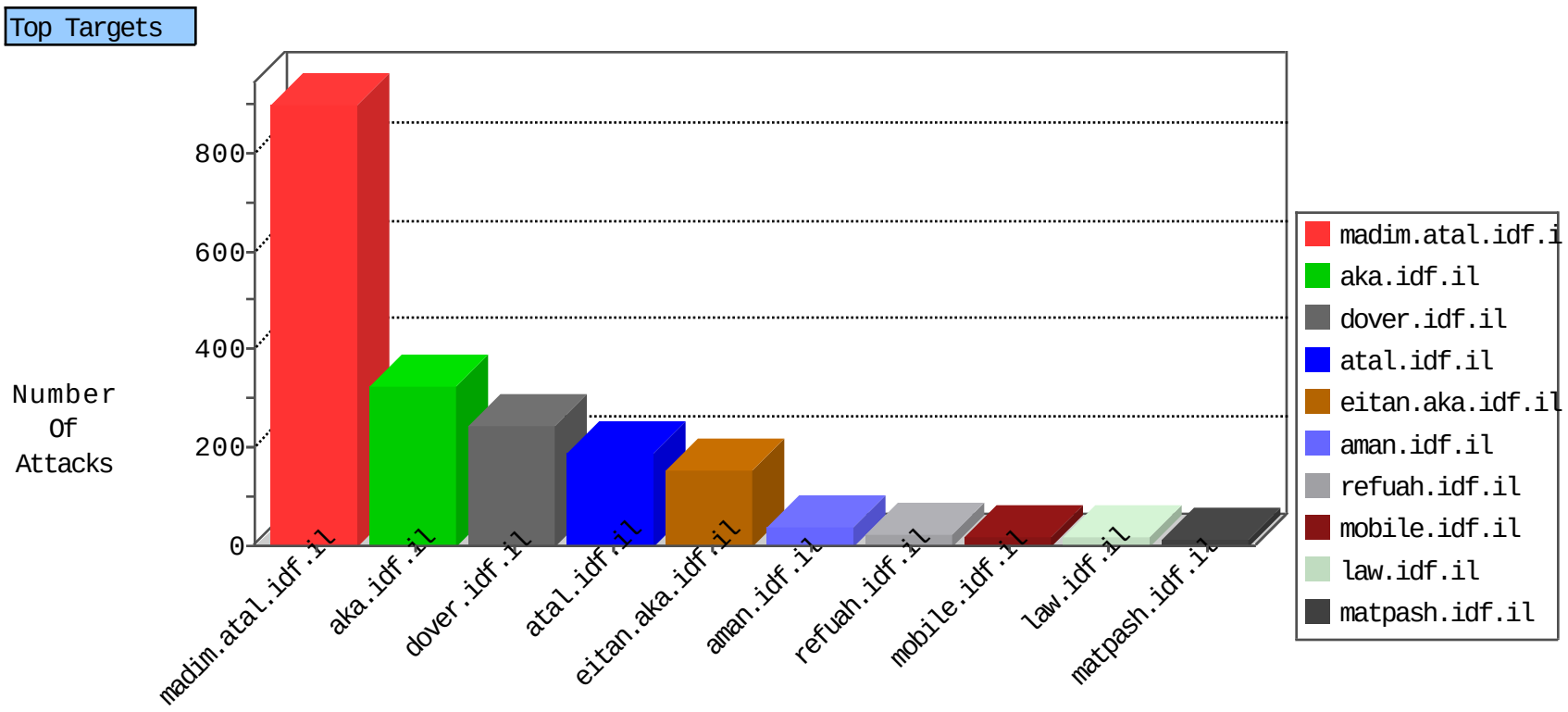
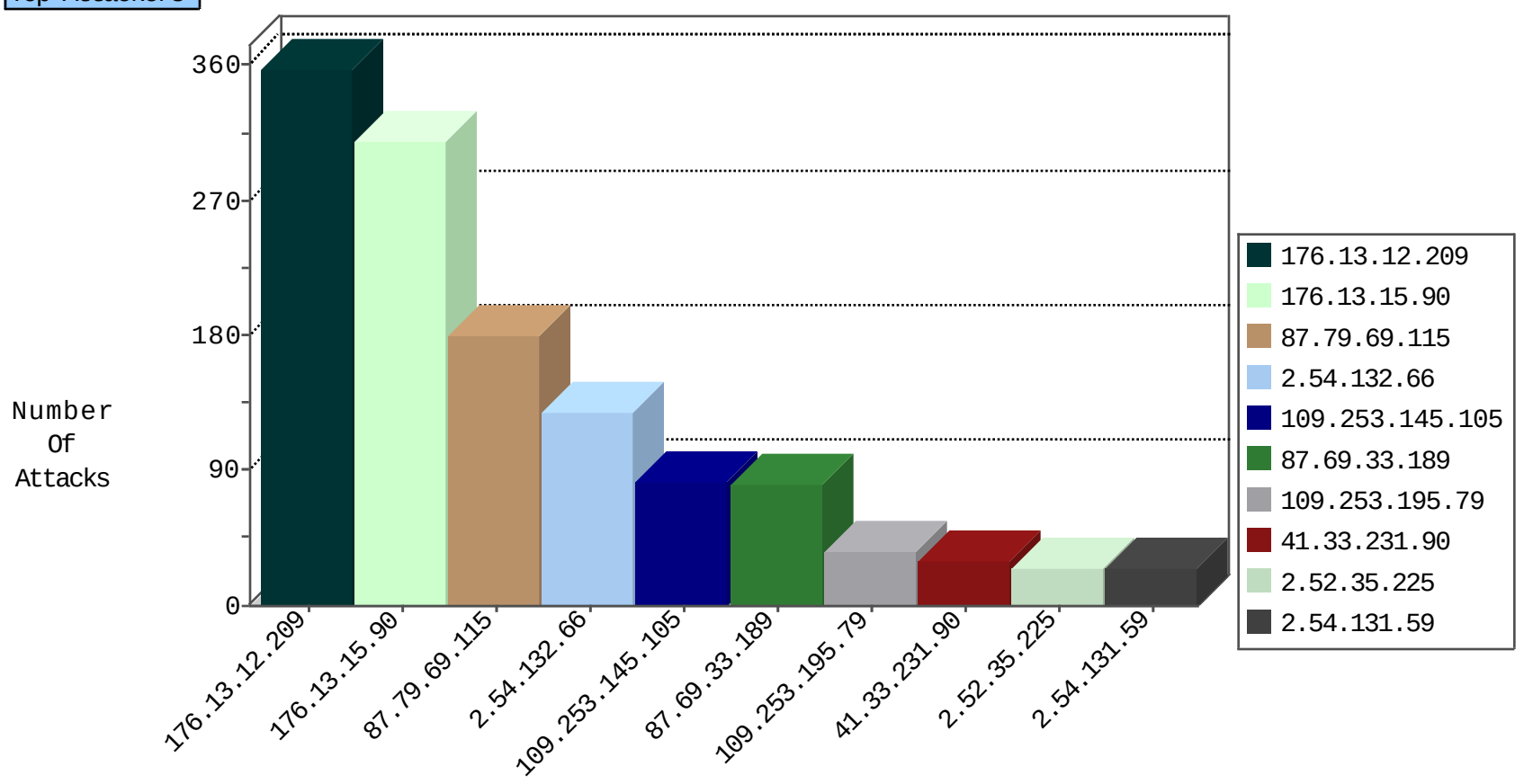
02-16-2016-21:04:07 to 02-16-2016-22:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-16-2016-21:04:07 to 02-16-2016-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.81.202	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	17
37.59.28.127	France	147.237.76.44	e.refuah.idf.i	Block_Ntp_All_Net	drop	1
173.208.206.203	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1

02-16-2016-21:04:07 to 02-16-2016-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.102	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
144.76.8.132	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

02-16-2016-21:04:07 to 02-16-2016-22:04:07

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
185.130.5.179	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
157.55.39.72	147.237.0.34	United States	tikshuv.idf.il	SERVER-IIS asp-dot attempt	1
94.159.159.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.117.83.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.121.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.114.105.254	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.130.5.179	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
149.78.54.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
46.117.130.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.27.197	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
218.57.11.7	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1

02-16-2016-21:04:07 to 02-16-2016-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.54.132.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	129
87.79.69.115	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	87
87.79.69.115	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.52.35.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
87.79.69.115	Germany	147.237.77.233	atal.idf.il	drop		drop	23
87.79.69.115	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence		monitor	21
166.137.242.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.8.240.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.148.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.59.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
2.54.131.59	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
37.26.149.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.120.126.106		147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
87.79.69.115	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	8
87.69.149.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
94.159.147.232	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
185.32.179.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.202.9	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.1	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.9.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.62.36	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.169.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
138.134.102.15	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.117.142.72	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.127.224.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
95.86.103.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.39.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.163.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.186.171.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.44.129.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.127.224.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.181.98.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
109.253.136.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
193.43.245.250	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	3
5.22.129.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.153.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-16-2016-21:04:07 to 02-16-2016-22:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	216
176.13.15.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	167
176.13.12.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	139
176.13.15.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.145.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
109.253.195.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.13.15.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	36
109.65.7.221	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.7.221	Block	13
5.28.186.167	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 5.28.186.167	Block	8
109.65.7.221	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	7
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.228.178.77	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
5.228.178.77	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.228.178.77	Block	5
79.176.149.120	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.149.120	Block	5
46.19.86.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	5
5.28.186.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed PHP Attempt	Block	4
2.54.12.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.149.120	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
31.168.14.82	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
178.137.17.196	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
46.19.85.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.26.122.212	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.57.226.144	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
109.253.145.105	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
5.28.186.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.253.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.127.174.249	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 77.127.174.249 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
84.228.6.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$71 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.136	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.136.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
94.159.147.232	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.127.174.249	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 77.127.174.249	Block	1
77.127.174.249	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
79.179.6.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$72 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
77.127.174.249	Israel	147.237.77.216	dover.idf.il	NULL Character in Method [[#2]]Â½Â«[[#25]]Ã€Â©'[[#25]]Y`(`Â?Ãƒ[[#30]]Ã‡[[#2]][[#25]]~%Â¶Ã‰Â†ÃžV[[#25]]Â‰Ã ÃŸcÃ³[[#31]]Â¦Â›Â^}Ã› ÂŠHÂ›sÃŽÃ—Ã¢9Ã-_[[#4]]Ã»Ãª•Ã˜Â§Ã-F[[#6]]Â'Ã“rL[[#23]][Ã† Â [[#26]]?[[#29]][[#17]]S(Â„t3Â°MÂ´Â³[[#2]]JÃ«GÃ¤[[#21]]Ã• Y44h)[[#24]]JÂ•Ã®\t?Ã‰+Â¨gÃ»Ã€Ã˜Ã¥Â§ÂŒÃ– Â?Ã¦[[#26]][[#14]]Ã¼ÃŽ[[#0]]Â‹([[[#26]]Ã¦}Â-4Â'Ã…	Block	1
87.69.49.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
77.127.174.249	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 77.127.174.249	Block	1
195.138.83.203	Ukraine	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
79.180.98.101	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.98.101	Block	1
77.127.174.249	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
46.19.86.220	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.19.86.220	Block	1
149.78.29.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 149.78.29.70	Block	1
77.127.174.249	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 77.127.174.249	Block	1
203.133.168.41	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
77.127.174.249	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 8	Block	1

02-16-2016-21:04:07 to 02-16-2016-22:04:07