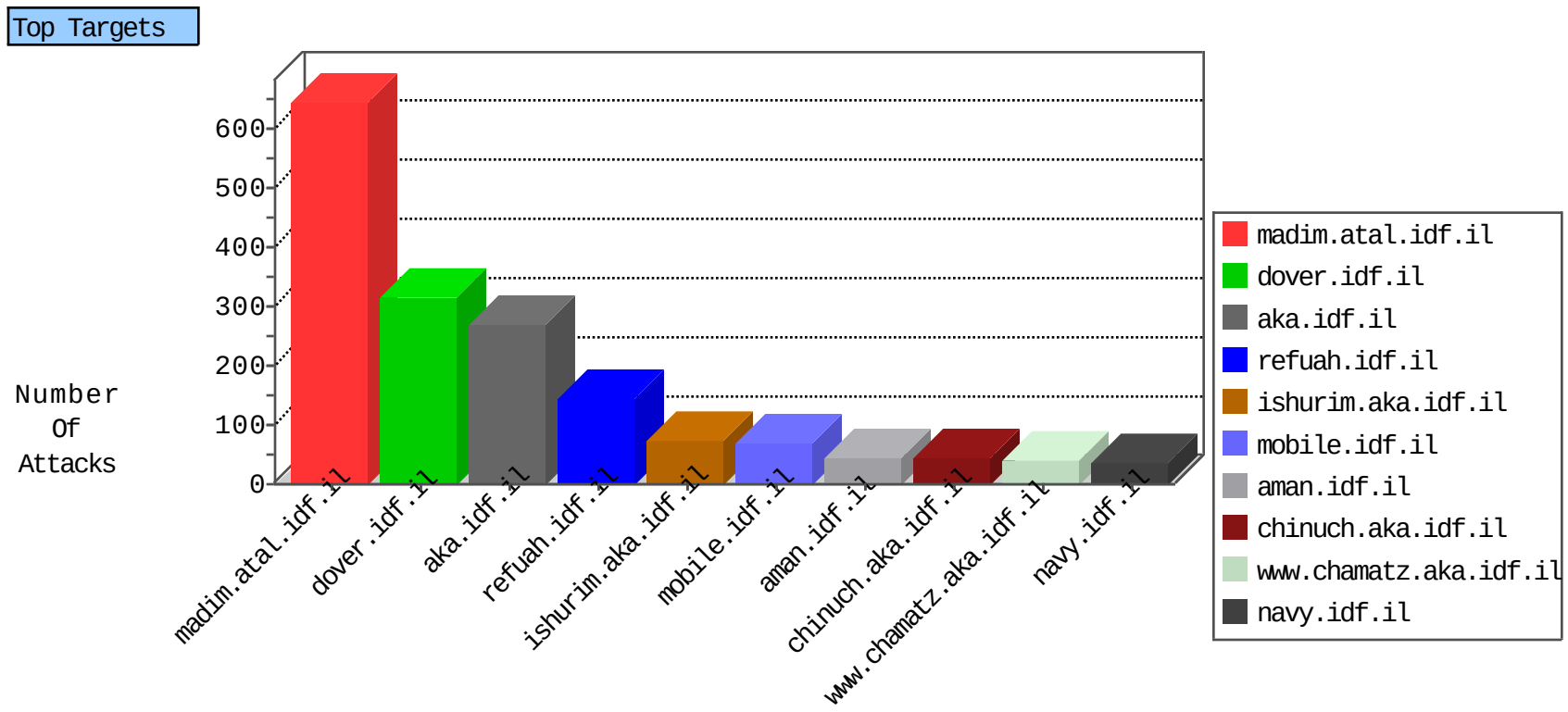
02-11-2016-15:04:06 to 02-11-2016-16:04:06

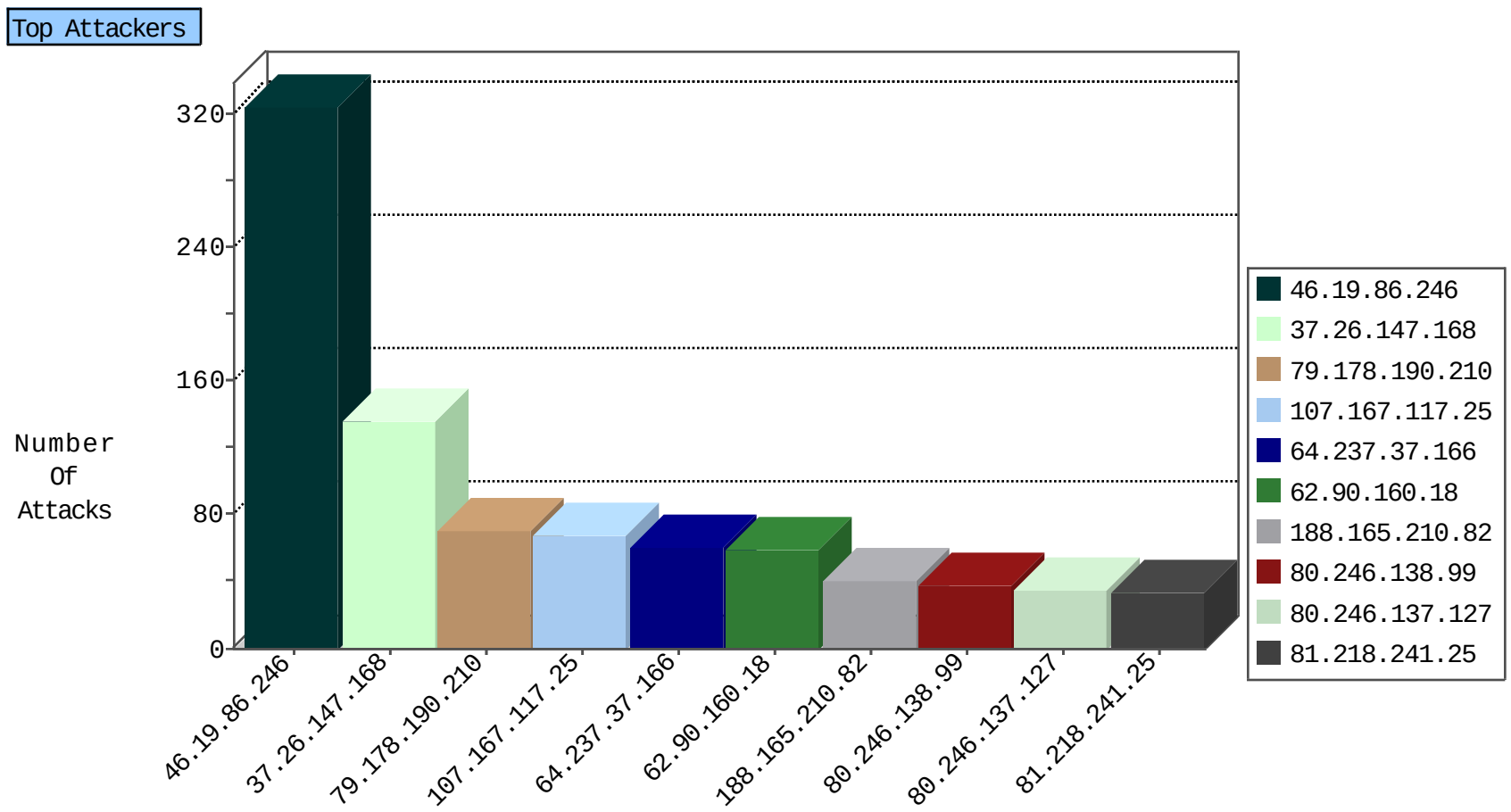
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-11-2016-15:04:06 to 02-11-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
84.108.22.169	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
69.31.51.104	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.253.156.120	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
212.235.27.129	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.117.136.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
115.239.228.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.94.111.1		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
31.220.4.161	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.130.5.228		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-15:04:06 to 02-11-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.216.115.8		147.237.77.216	dover.idf.i	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.i	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.210.82	France	147.237.77.216	dover.idf.i	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	1
213.239.205.66	Germany	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1

02-11-2016-15:04:06 to 02-11-2016-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.165.210.82	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.19.85.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.67.206.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
108.4.93.186	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.117.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
69.31.51.104	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.221.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.121.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.98.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1

02-11-2016-15:04:06 to 02-11-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.117.25	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	68
79.178.190.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
62.90.160.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
2.52.136.26	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
64.237.37.166	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
64.237.37.166	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
141.0.11.60	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
46.19.85.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
37.26.147.168	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	14
17.78.79.134	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.212	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.62.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.147.168	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.108.22.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.89.217.230		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.37	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.168	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.190.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.164.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.135.102.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.190.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.147.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.135.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.243.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.229		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
5.29.235.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.10.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.153.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.235		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
149.78.227.4	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
192.115.200.93	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
84.108.22.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.62.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.145.220.192	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.62.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.71.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.62.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
109.186.132.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.227		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
2.54.62.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.179.9.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.118.12.102	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
213.8.204.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.78.254	United States	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.69.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

02-11-2016-15:04:06 to 02-11-2016-16:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.246	Block	67
37.26.147.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
37.26.147.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
80.246.138.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
80.246.137.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
109.253.216.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
37.26.147.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
80.246.137.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
188.165.210.82	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	15
84.228.227.13	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.227.13	Block	15
188.165.210.82	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.210.82	Block	14
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	8
80.246.137.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
64.71.32.32	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.71.32.32	Block	5
80.246.137.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	4
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
37.26.147.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.202.194	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
213.239.205.66	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.239.205.66	Block	3
2.54.62.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.142.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.43.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
84.108.92.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
46.19.86.238	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
188.165.210.82	France	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 188.165.210.82	Block	2
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.26.188.232	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Header Name	Block	1
109.253.140.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.3.95	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
84.108.22.169	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method Âº[[#4]]7GoÃ‡Ã›Ã¯Â?S2qEÃ»ÃˆÂ¸ in URL	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl95 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
212.143.110.33	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
54.67.110.194	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
95.86.114.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/,	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Unknown HTTP Request Method Â€#FÂ¯Ã˜Ã™Â¢Â‰0Ã?eÂ”•Ã œÂ¹PÂƒÃ¥Â™Â·ka"[[#29]]Ã¹Ã?![[#23]]GÃ¬ in URL	Block	1
79.177.162.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/register/mailingsignup.asp	Block	1
31.220.4.161	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL	Block	1
64.71.32.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
198.46.101.11	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
176.13.11.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1

02-11-2016-15:04:06 to 02-11-2016-16:04:06