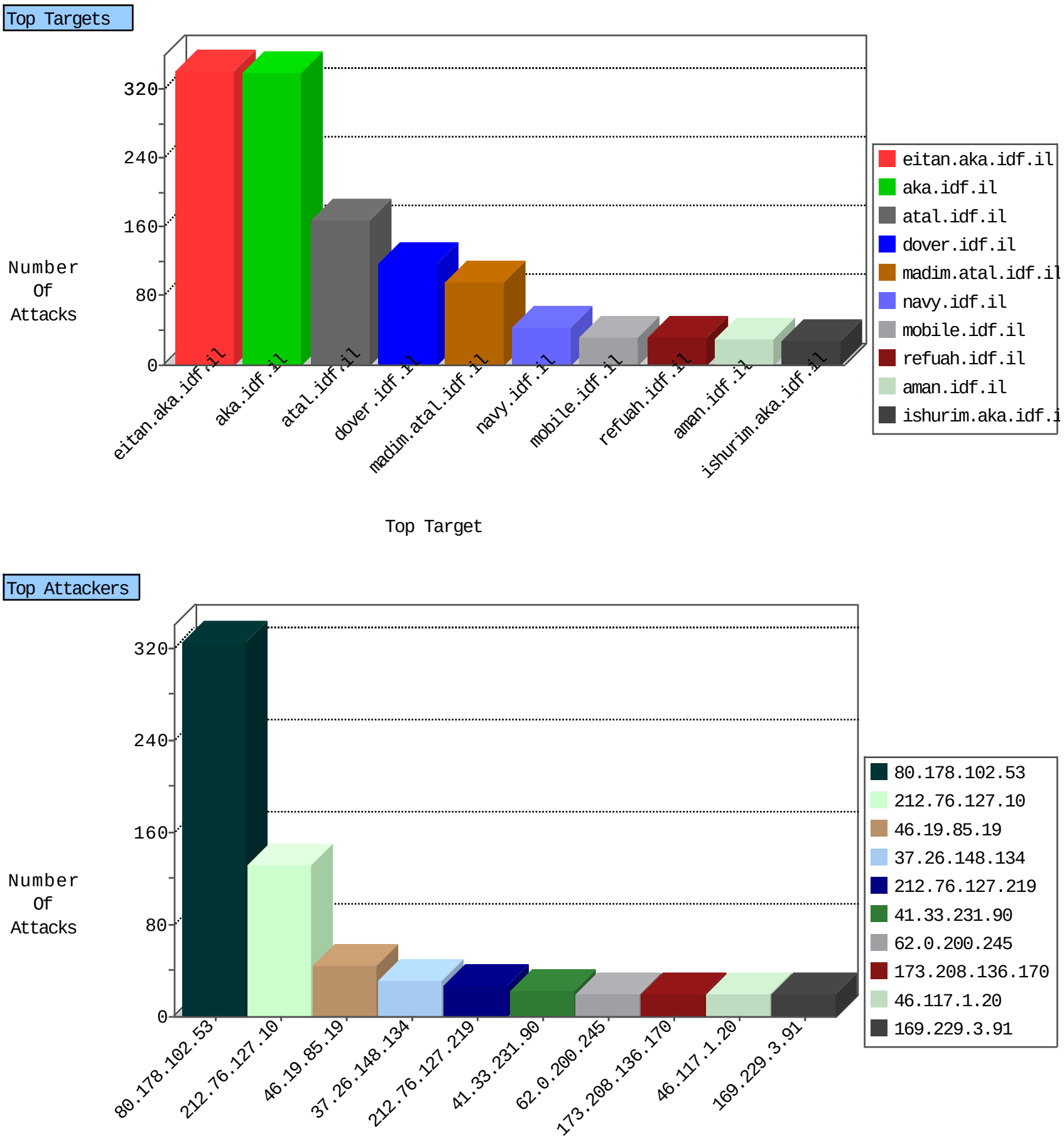
02-16-2016-16:04:06 to 02-16-2016-17:04:06

IDF Under Attack Daily Report



02-16-2016-16:04:06 to 02-16-2016-17:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	204
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
31.168.213.161	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
173.208.206.205	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
66.240.236.119	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
173.208.206.203	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1

02-16-2016-16:04:06 to 02-16-2016-17:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.44.142.202	Israel	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	1
46.120.204.172	Israel	147.237.77.170	maarachot.idf.il	C008: HTTP: Xenu UserAgent	Block	1
46.120.204.172	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-16-2016-16:04:06 to 02-16-2016-17:04:06

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	2
5.236.217.192	147.237.76.39	Iran, Islamic Republic of	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
118.193.156.149	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
93.173.146.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.110.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.58.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.197.145.242	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
67.81.250.171	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.12.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.254.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.198.151.36	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.187.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.22.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.182.17.13	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 4096	1
87.71.19.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.192.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.197.145.242	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.57.223.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.210.187.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

02-16-2016-16:04:06 to 02-16-2016-17:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.178.102.53	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	325
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	132
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
62.0.200.245	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
79.180.21.172	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
173.208.136.170	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
46.19.86.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
132.64.25.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.58.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.241.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.64.215.69	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.130.227.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.106.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
31.210.187.31	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
95.86.106.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.210.187.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.227.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.203.122.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.3.146.244	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
85.65.106.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
62.0.116.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.13.2.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.144.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.110.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.12.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.175.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.203.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.126.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.2.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.227.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.165.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.28.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.214.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.33.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.255	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-16-2016-16:04:06 to 02-16-2016-17:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.178.208.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-16-2016-16:04:06 to 02-16-2016-17:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
37.26.148.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
5.29.199.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
46.117.1.20	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.117.1.20	Block	9
185.32.179.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
84.108.218.123	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.108.218.123	Block	7
176.13.1.174	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/994-8516-he/himush.aspxâ€?â€Ž	Block	7
46.117.1.20	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	5
173.208.136.170	United States	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	4
84.108.218.123	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	4
46.116.127.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.52.39.214	Israel	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 2.52.39.214	Block	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	3
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
80.246.137.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.185.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
193.109.196.41	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1498-en/dover.asp	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.168.67.53	Block	2
85.65.17.228	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.17.228	Block	2
149.78.190.220	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.190.220	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
213.151.48.226	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 213.151.48.226	Block	1
95.86.84.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/dover.aspx&sa=u&ved=0ahukewir_-djxvzkahufthqkhfz-bbmqfggqma4&usg=afqjcnepjiaix3qorrzujiwlvwkx6xrmsw	Block	1
37.26.147.135	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.183.22.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.132.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$11 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Â™ [[#22]][[#4]]A}[[#21]]q[[#24]]y0ÃŸÃ³?[[#5]]>;Â¿5ÃŒÃ·Ã‡Ã°ÂŸ[[#3]]	Block	1
149.78.40.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.117.1.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ajax/updatestatus.php	Block	1
212.199.198.120	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.228.226.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
80.178.102.53	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/×ž×?×™ ×¨ ×©×—×ž×•×Ÿ.aspx	Block	1
2.52.161.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
149.78.190.220	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1391-12402-en/dover.aspx	Block	1
95.86.106.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.147.183	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3259.jpg	Block	1
79.183.128.217	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
2.54.132.166	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$119 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â‹_Â…LtÂ zÂ³Â¿	Block	1
149.78.40.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.120.7.249	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
212.199.198.123	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.228.226.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$76 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
198.204.249.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	NULL Character in Method	Block	1
80.230.25.52	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	1

02-16-2016-16:04:06 to 02-16-2016-17:04:06