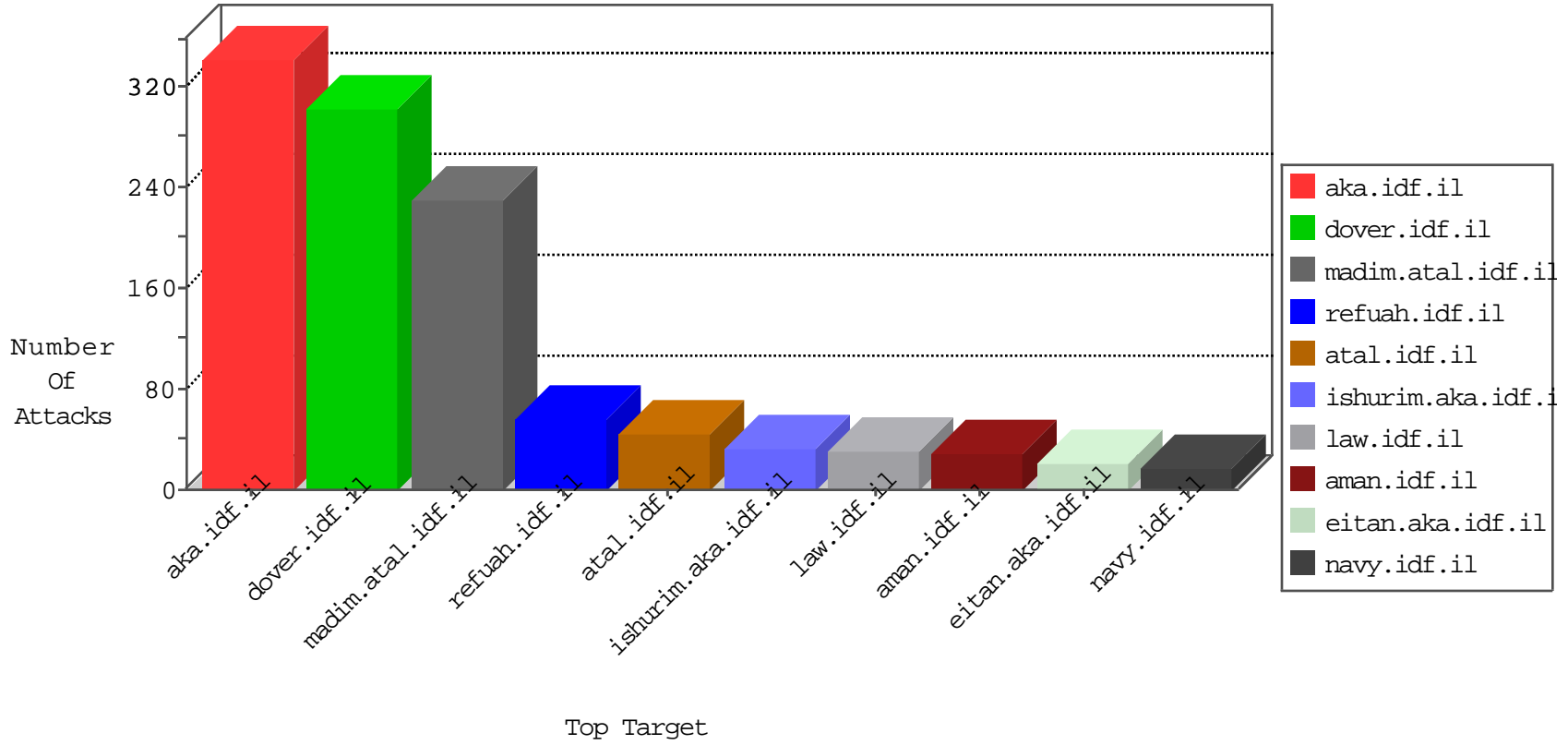


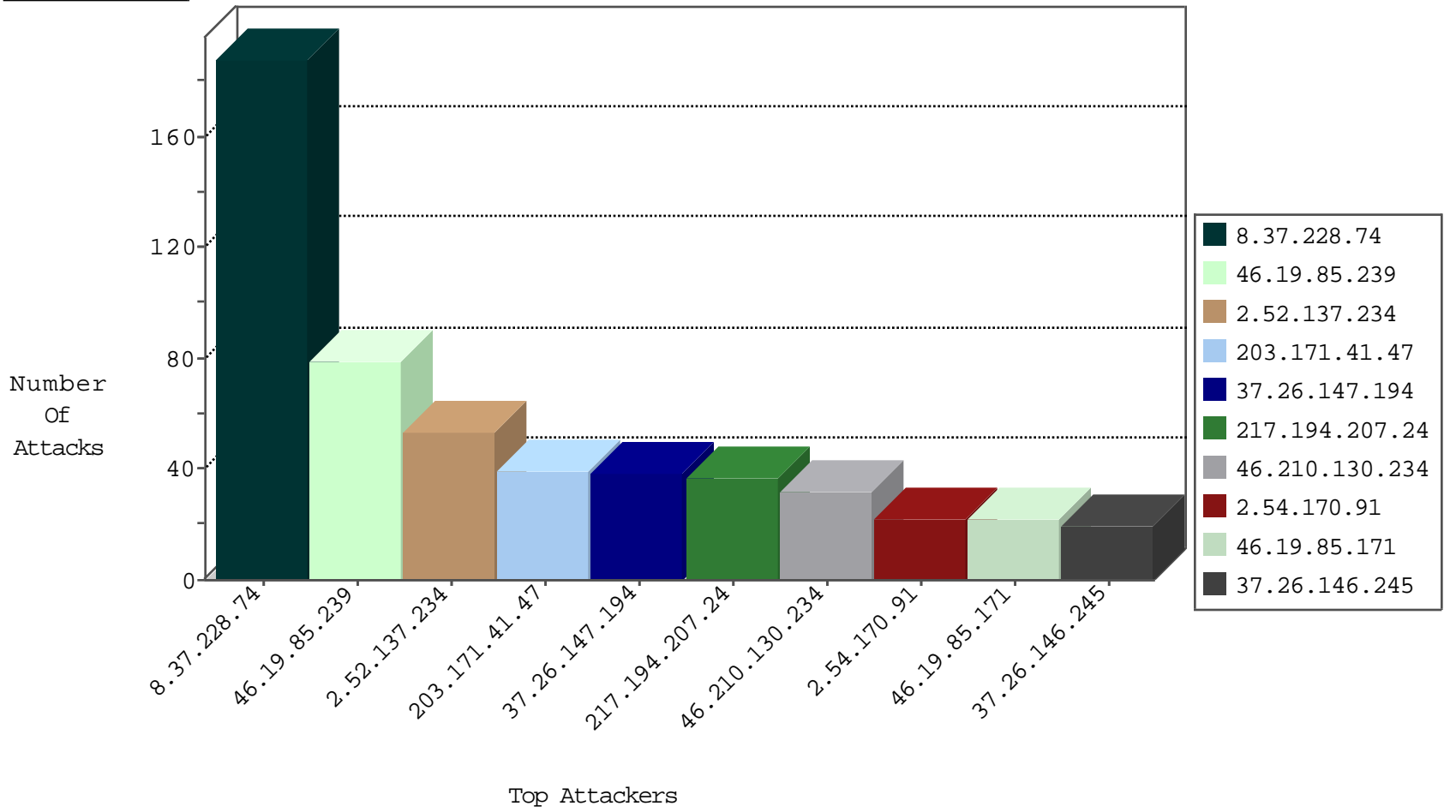
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
173.208.206.202	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
5.39.218.13	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
173.208.206.202	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
173.208.206.202	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
203.171.41.47	New Zealand	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
203.171.41.47	New Zealand	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
203.171.41.47	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	21
203.171.41.47	147.237.77.233	New Zealand	atal.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	3
203.171.41.47	147.237.77.233	New Zealand	atal.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	3
79.179.62.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.27.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.221.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.205.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.21.131	147.237.8.14	Israel	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.178.143.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.31.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.76.106.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
110.247.249.235	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.111.36.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.251.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.228.74	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
8.37.228.74	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	87
217.194.207.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
2.54.170.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.86.213	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
109.253.144.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
217.194.207.24	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
85.130.231.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.103.252	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.74.38.14	Sweden	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	11
176.13.2.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.31.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
79.181.174.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.171	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.158.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.168.99	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.142	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.1.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.108	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
171.48.48.250	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.108	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.57.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.171	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.150.196.70	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
134.213.209.30	United Kingdom	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
199.30.24.22	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.146.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
171.48.48.250	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.219.114.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.250.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.66.100.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.55.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.22.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.117.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.113.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-16-2016-10:04:02 to 02-16-2016-11:04:02

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
2.52.137.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
37.26.147.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.210.130.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
2.54.159.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
213.57.7.4	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.57.7.4	Block	9
46.19.86.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
176.13.23.84	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
79.183.220.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.183.220.77	Block	3
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.183.220.77	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
46.19.86.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$35 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.15.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
37.26.147.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$42 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
142.160.241.91	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.52.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.168.21.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.19.198	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
79.181.174.34	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
2.54.137.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.65.189.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
213.57.7.4	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/2/size338x0/1802.jpg	Block	1
2.54.16.29	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$67 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
183.240.92.136	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
172.100.224.83		147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
77.127.133.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
2.54.53.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$90 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
87.69.128.183	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$21 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
195.200.205.22	Israel	147.237.77.226	www.chamatz.aka.i df.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
2.52.158.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
80.246.136.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$76 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.21.117	Israel	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
2.54.156.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.253.138.233	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
213.57.158.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$41 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.31.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$101 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.158.133	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
37.26.148.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$71 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
183.240.92.137	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.28.170.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestio n\$7 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
172.100.224.83		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
77.127.182.173	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1

02-16-2016-10:04:02 to 02-16-2016-11:04:02

02-16-2016-10:04:02 to 02-16-2016-11:04:02