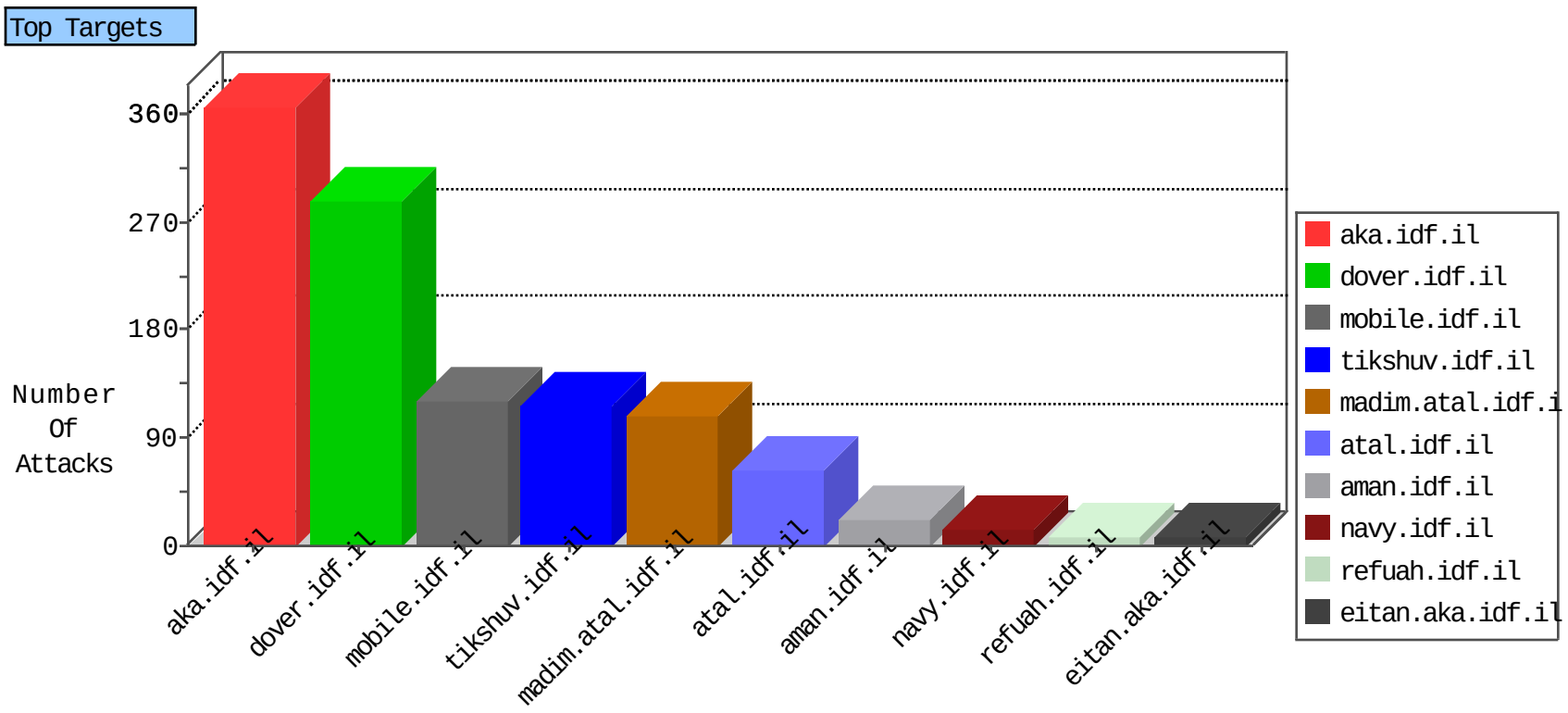
02-03-2016-19:04:08 to 02-03-2016-20:04:08

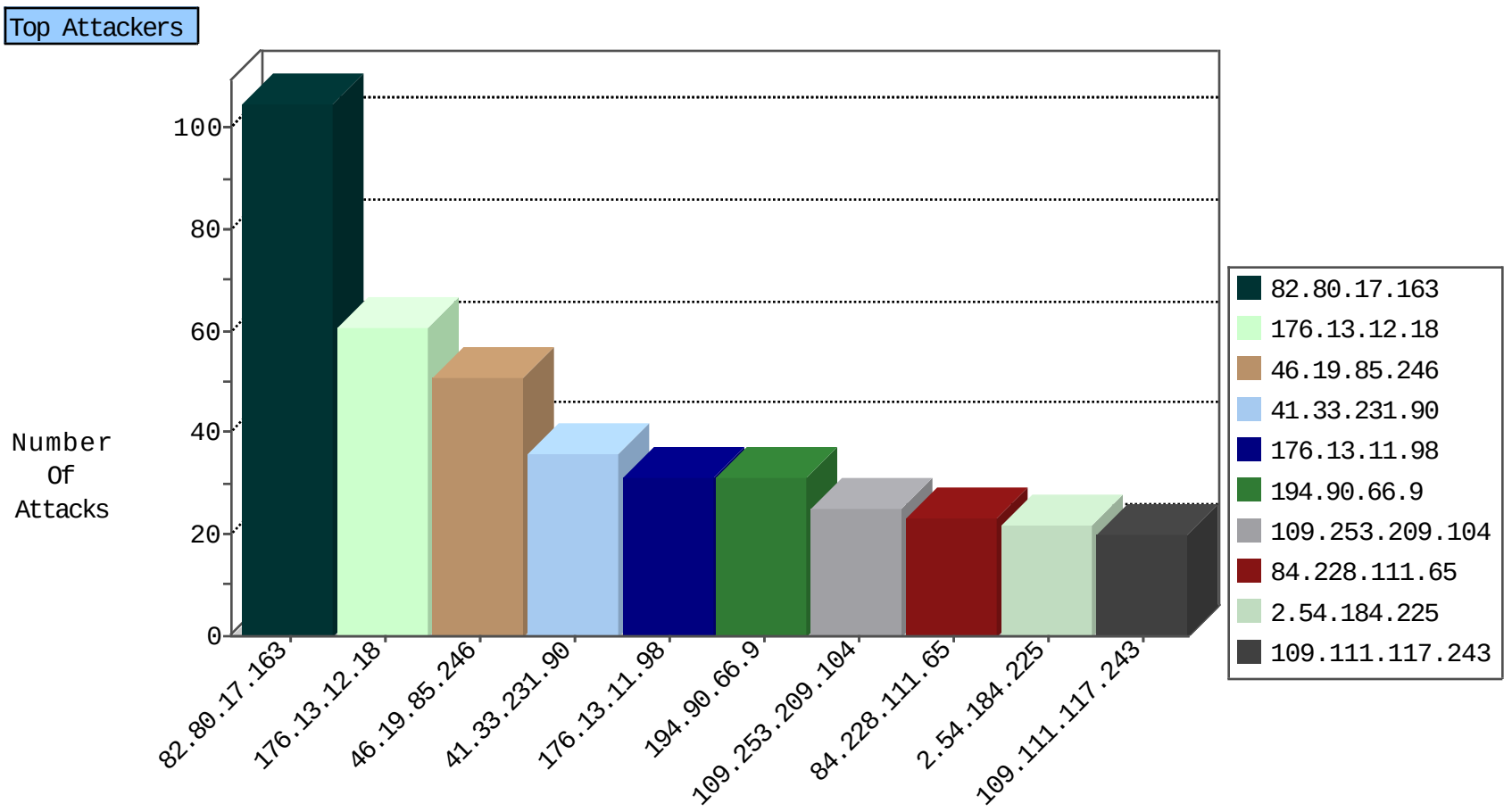
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-03-2016-19:04:08 to 02-03-2016-20:04:08

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	12
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
89.248.160.138	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
68.116.5.134	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
159.122.252.41	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

02-03-2016-19:04:08 to 02-03-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.188.157	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
212.83.177.193	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
5.196.129.51	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
88.150.221.26	United Kingdom	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-03-2016-19:04:08 to 02-03-2016-20:04:08

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	3
123.201.255.106	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
109.235.254.181	147.237.72.14	Turkey	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
185.120.125.49	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.72.14	Turkey	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.81.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.201.255.106	147.237.77.234	India	halag.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.148	Canada	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
123.201.255.106	147.237.76.30	India	himush.idf.il	ET SCAN Potential SSH Scan	1
95.90.254.102	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
123.201.255.106	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.176.194.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.201.255.106	147.237.0.200	India	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.23.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
123.201.255.106	147.237.0.33	India	idf.il	ET SCAN Potential SSH Scan	1
37.26.146.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
123.201.255.106	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.72.14	Turkey	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
176.13.11.98	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
109.160.240.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
124.244.142.148	147.237.0.33	Hong Kong	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.168.133.63	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
123.201.255.106	147.237.76.34	India	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.148	Canada	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
123.201.255.106	147.237.72.167	India	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.81	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.201.255.106	147.237.8.27	India	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.127.114.18	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.201.255.106	147.237.0.34	India	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.72.217	United States	e.idf.il	ET DROP Dshield Block Listed Source	1

02-03-2016-19:04:08 to 02-03-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.246	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
194.90.66.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
84.228.111.65	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
107.167.105.143	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.85.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
176.13.11.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
176.13.11.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
176.13.11.195	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.118.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
79.181.17.73	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.209.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
31.210.187.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.209.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.111.117.243	Andorra	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
185.3.144.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.50	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.162.14.14	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.38.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.110.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.246	Israel	147.237.77.243	mobile.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.125.42		147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
109.66.51.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.209.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.205.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.111.117.243	Andorra	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
31.210.187.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.111.117.243	Andorra	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
2.54.185.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.147.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.111.117.243	Andorra	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.133	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.43.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.133	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.146.103	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.226.48.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.18.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

02-03-2016-19:04:08 to 02-03-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.17.163	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 82.80.17.163	Block	105
176.13.12.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.54.184.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
37.26.149.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
89.138.124.218	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 89.138.124.218	Block	6
176.13.12.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
176.13.11.195	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.246.137.32	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
2.54.31.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.86.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.86.219	Block	3
89.138.124.218	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
2.54.8.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
93.173.183.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$98 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
176.13.13.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
79.181.17.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.40.39	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation txtContent in www.tikshuv.idf.il/modules/forums.frm/frmmessage.aspx	Block	2
84.110.7.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$100 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
149.78.202.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	2
185.3.147.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.142.214.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.46.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.64.25.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$14 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
87.68.52.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.178.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.110.7.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
37.142.180.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/1705.jpgï»¿	Block	2
84.108.100.205	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$79 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.120.164.166	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.78.149.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$4 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
80.246.137.229	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.57.128.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl04.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
41.250.117.29	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
31.210.187.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.54.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
195.150.48.40	Poland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.79	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/templatecontrols/news/www.google.com	Block	1
2.54.189.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$58 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
84.240.36.40	Lithuania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.249	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.253.193.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$75 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
81.221.26.26	Switzerland	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
209.88.157.203	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
37.142.214.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
89.138.121.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$112 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
86.99.44.112	United Arab Emirates	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
77.125.101.222	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59390&docid=59518	Block	1

02-03-2016-19:04:08 to 02-03-2016-20:04:08

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.163.89	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in aka.idf.il/main/giyus/questionnaire.aspx	None	1

02-03-2016-19:04:08 to 02-03-2016-20:04:08