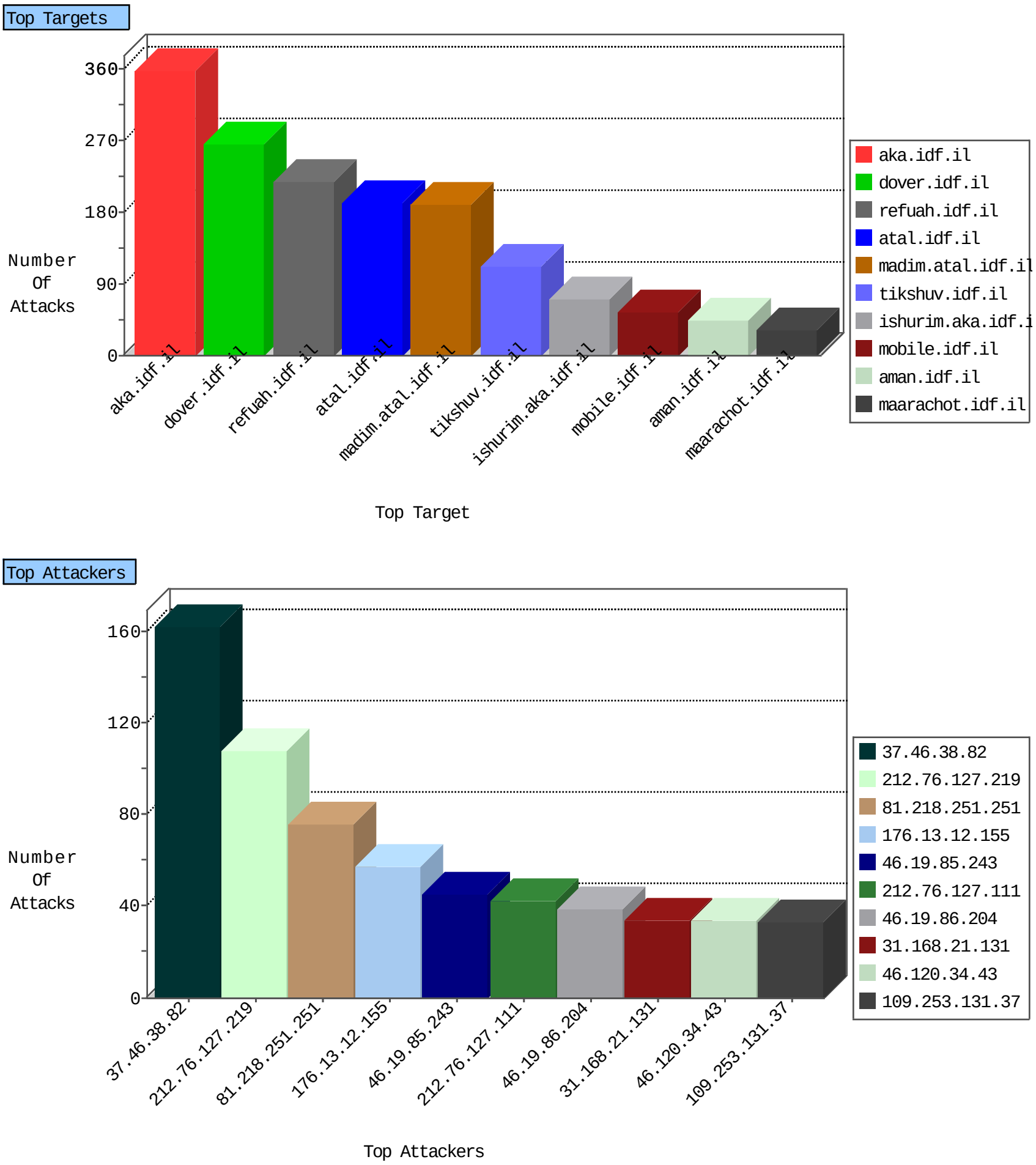
02-15-2016-13:04:02 to 02-15-2016-14:04:02

IDF Under Attack
Daily Report



02-15-2016-13:04:02 to 02-15-2016-14:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.222.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.19.86.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
216.72.40.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
185.32.179.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.80.217.70	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
176.13.4.224	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
41.236.215.66	Egypt	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
93.158.203.154	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
93.158.203.154	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

02-15-2016-13:04:02 to 02-15-2016-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-15-2016-13:04:02 to 02-15-2016-14:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	31
66.249.79.108	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
58.177.56.225	147.237.8.24	Hong Kong	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.121.27.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.120.125.38	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1
77.174.25.173	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
50.117.45.78	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.18.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.126.77.138	147.237.0.33	Sweden	idf.il	ET SCAN NMAP -sS window 1024	1
176.13.21.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.145.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-15-2016-13:04:02 to 02-15-2016-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.46.38.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	161
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	108
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	42
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	29
81.218.89.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
109.253.131.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
27.123.171.222	Fiji	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
2.54.169.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.10.173	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.199	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.149	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
31.168.21.131	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	10
46.19.85.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.228.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.147.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.21.131	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	9
46.19.86.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.254	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.66.107	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.85	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
79.180.134.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
80.246.137.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.11.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.149.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.228.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.18.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.87.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.237.234.103	Slovakia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.149.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.145.0	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.168.21.131	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.198.164	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.149.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.168.21.131	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
37.26.149.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

02-15-2016-13:04:02 to 02-15-2016-14:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.251	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
176.13.12.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.120.34.43	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
80.246.137.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.131.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 52.48.22.169	Block	5
109.186.163.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	5
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 52.48.22.169	Block	5
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 52.48.22.169	Block	5
207.46.13.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
52.48.22.169	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 52.48.22.169	Block	5
109.253.141.1	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.141.1	None	4
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	4
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
62.219.229.226	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
2.54.32.141	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.139.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.52.60.0	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
2.54.170.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsP in aka.idf.il/main/sachar/viewpayslip.aspx	None	1
46.120.34.43	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
212.179.1.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$42 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.30.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl71 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
41.236.215.66	Egypt	147.237.77.216	dover.idf.il	Automated Vulnerability Scanning	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20329-he/dover.aspx	Block	1
2.54.170.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDFFor in aka.idf.il/main/sachar/viewpayslip.aspx	None	1
84.94.174.21	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
217.132.152.198	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in URL	Block	1
2.54.170.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter I in aka.idf.il/main/sachar/viewpayslip.aspx	None	1
80.246.137.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9692-he/refuah.aspx	Block	1
37.26.149.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.170.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter Sli in aka.idf.il/main/sachar/viewpayslip.aspx	None	1
2.54.170.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPD in aka.idf.il/main/sachar/viewpayslip.aspx	None	1
52.48.22.169	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name user-Agent	Block	1
46.19.85.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sahar	Block	1
80.246.130.6	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19825-he/dover.aspx	Block	1
2.54.170.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter IsPDFForm in aka.idf.il/main/sachar/viewpayslip.aspx	None	1
84.94.182.226	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1

02-15-2016-13:04:02 to 02-15-2016-14:04:02