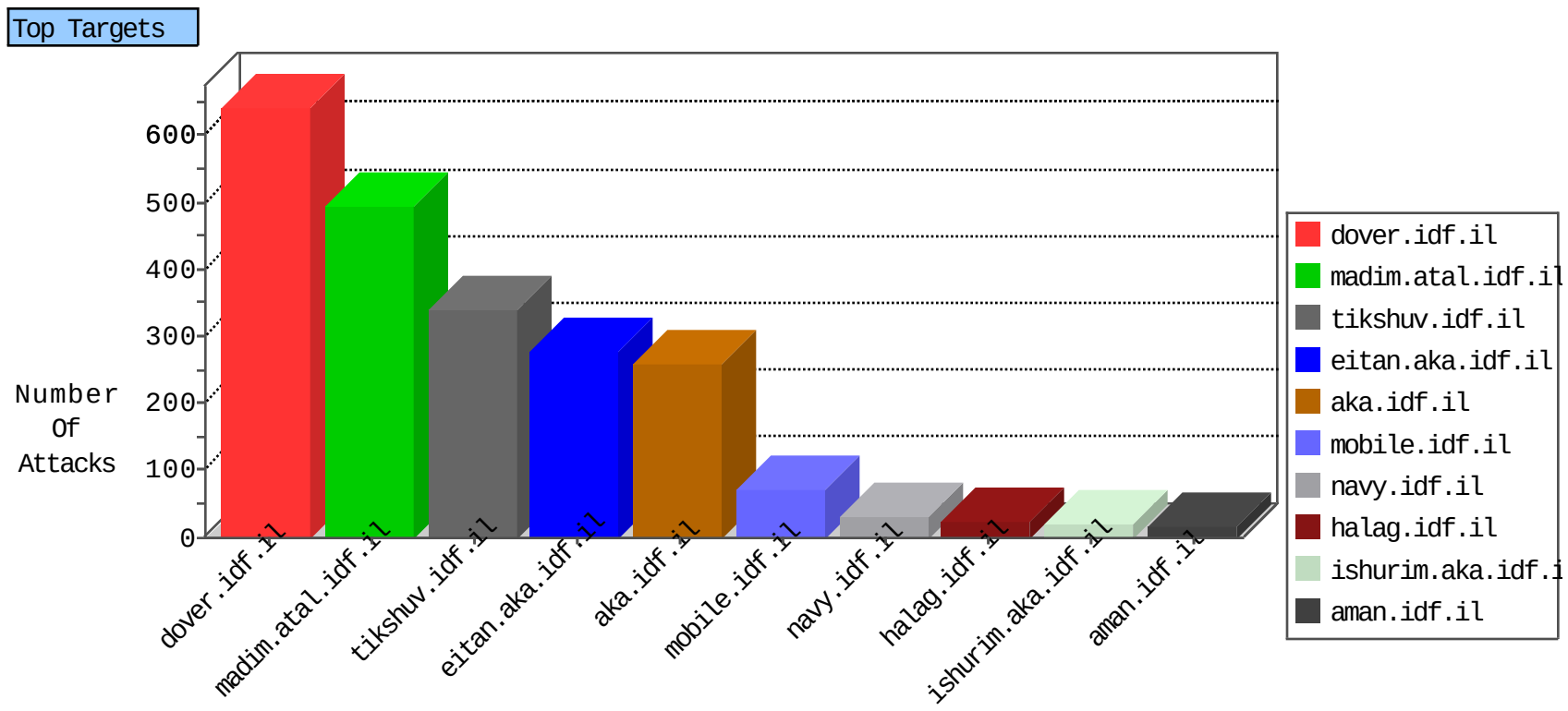
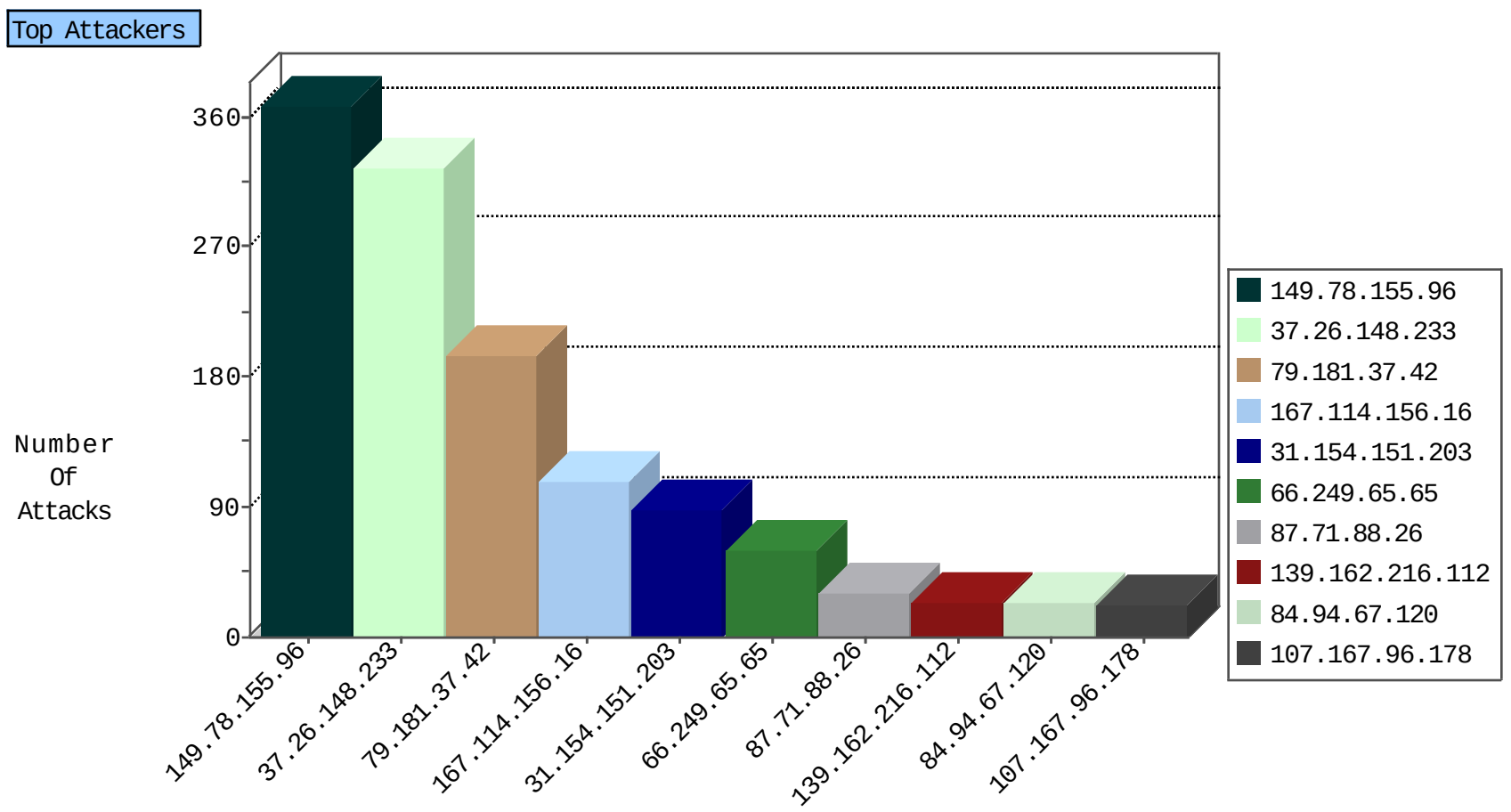
05-03-2016-18:04:08 to 05-03-2016-19:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-18:04:08 to 05-03-2016-19:04:08

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-POST-Segmented-DoS	dest-reset	2916
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2868
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
79.178.98.23	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
94.102.52.10	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
71.6.146.185	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-18:04:08 to 05-03-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-18:04:08 to 05-03-2016-19:04:08

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
79.178.160.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.105.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
149.88.35.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.190.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.209.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
2.53.158.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.54.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.12.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
81.218.175.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
79.180.138.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.30.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.65.167	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.88.236.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.138.139.178	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
115.47.12.162	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
37.46.38.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.142.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.160.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.52.47	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.33.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.70.33.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.232.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
80.246.136.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-03-2016-18:04:08 to 05-03-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.148.233	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	325
79.181.37.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	195
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
87.71.88.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
107.167.96.178	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
84.94.67.120	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
79.179.242.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.199.84.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
108.21.101.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
24.229.110.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
75.150.116.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.53.44.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.228.249.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.220.96	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.225.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
103.252.200.190	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.81.218	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.120.77.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.225.149	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.109.44.17	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.81.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.179.218.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.8.118.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.36.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.240	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.135.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.153.130.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.210.179.91	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.209.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.163.61.14	United Kingdom	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.179.143.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

05-03-2016-18:04:08 to 05-03-2016-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.155.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	368
31.154.151.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
109.253.193.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
64.60.9.178	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 64.60.9.178	Block	11
131.253.25.252	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.53.48.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.44.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
95.35.140.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.12.62	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.70.59.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
81.218.145.152	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.145.152	Block	2
173.251.20.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.65.167	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
81.218.145.152	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/faq/mobile	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.199	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
106.38.241.106	China	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.176.26.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
109.253.222.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
37.142.68.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.94.67.120	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
208.105.66.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.209.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	1
106.186.113.132	Japan	147.237.77.233	atal.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
79.181.9.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/סוג'א	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3048.jpg	Block	1
69.112.148.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.60.9.178	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/tfasim.aspx	Block	1
213.57.183.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.206.88.106	Russian Federation	147.237.77.19	law-forum.idf.il	Suspicious Response Code	Block	1
106.186.113.132	Japan	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3048.jpg	Block	1
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.138.70.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
71.251.19.27	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.253.135.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3044.jpg	Block	1
77.126.62.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

05-03-2016-18:04:08 to 05-03-2016-19:04:08