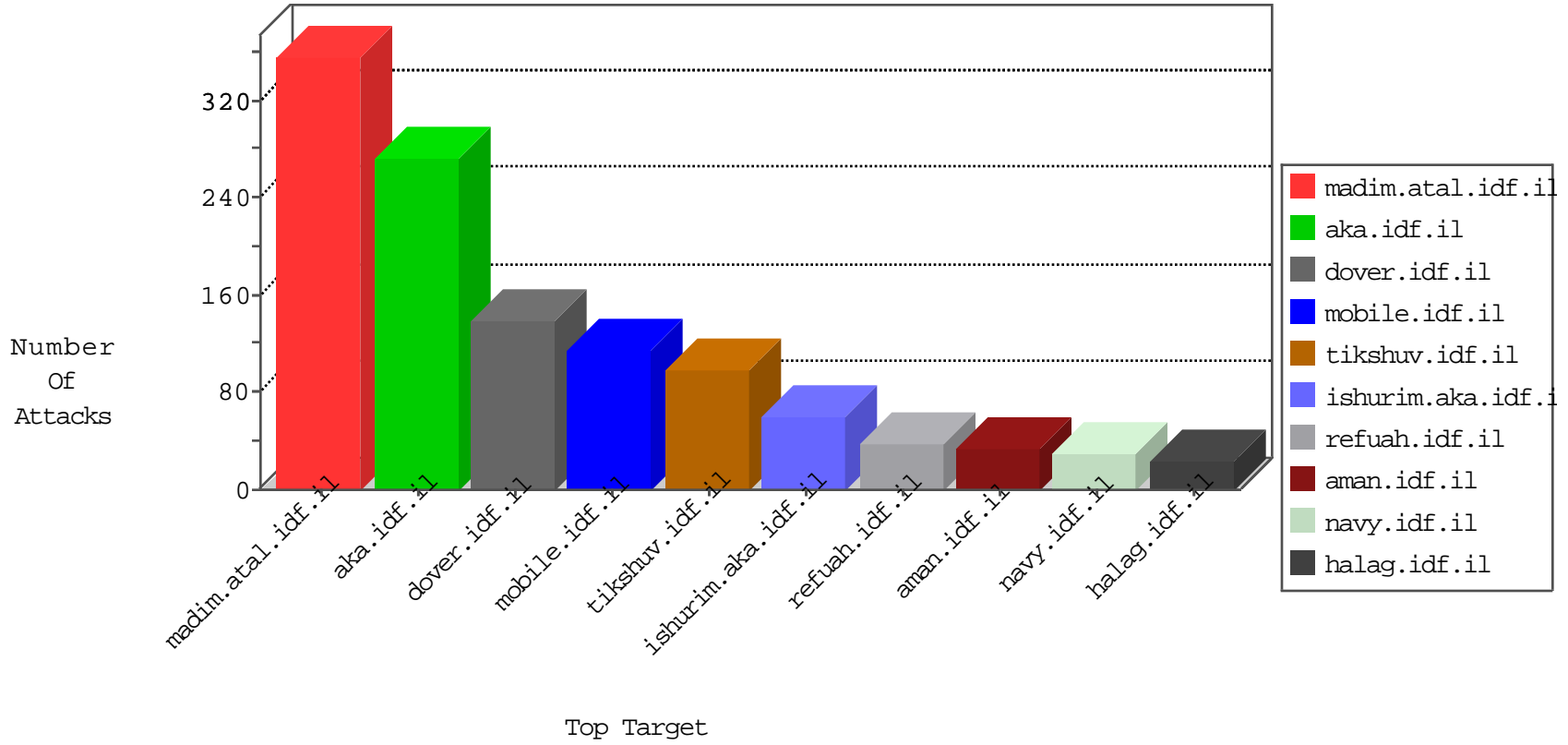


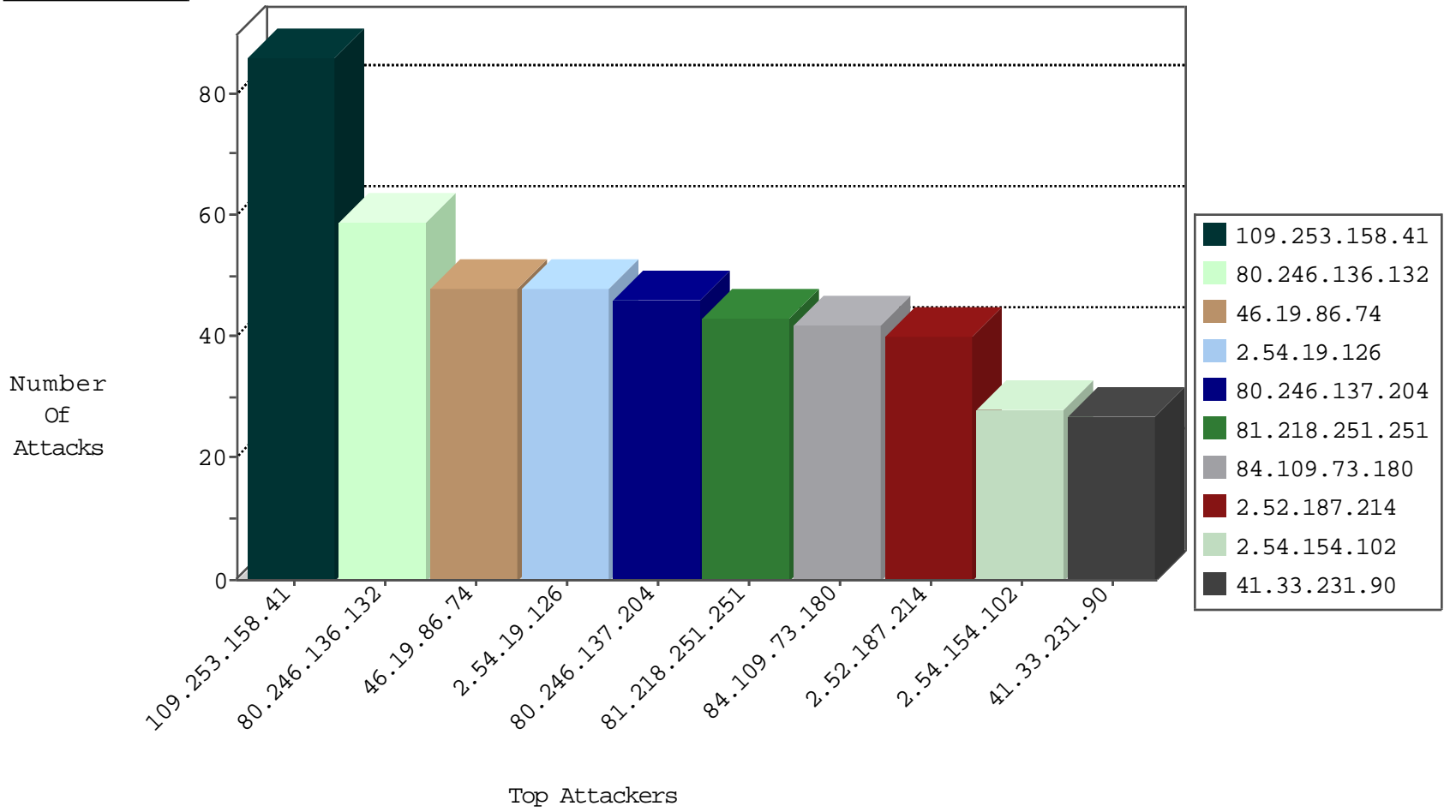
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
0.0.0.0		147.237.77.216	doover.idf.il	HTTP Page Flood Attack	drop	4
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

02-03-2016-10:04:08 to 02-03-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.8.63.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
189.254.90.133	147.237.72.167	Mexico	ishurim.aka.idf.i	ET SCAN NMAP -sS window 4096	1
189.254.90.133	147.237.72.167	Mexico	ishurim.aka.idf.i	ET SCAN NMAP -f -sS	1
176.228.167.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
147.235.185.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.39.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
212.25.106.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
189.254.90.133	147.237.72.167	Mexico	ishurim.aka.idf.i	ET SCAN NMAP -sS window 2048	1
188.120.135.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.229.106.59	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.81.193.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.254.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.187.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
79.180.125.131	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.85.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.85.115	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
2.54.154.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
80.246.136.132	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
176.13.5.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.132	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
2.54.173.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.172.114	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
81.218.241.25	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
212.117.143.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
195.160.242.40	Israel	147.237.72.166	aka.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
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.3.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
79.182.190.32	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.219.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.16.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.115	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.144.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.5.198	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.30.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.114.2	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
193.124.251.210	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.54.161.203	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.133.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.132	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	5
149.78.181.184	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
81.218.176.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
199.203.215.1	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.54.154.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.226.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.170.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.167.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.3.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.134.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.30	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
109.253.158.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.86.74	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
2.54.19.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
80.246.137.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
81.218.251.251	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
84.109.73.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
80.246.137.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
80.246.136.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
80.246.136.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
109.253.207.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.52.187.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
84.108.129.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.129.35	Block	6
46.19.85.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.241.201.65	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.241.201.65	Block	4
84.111.200.154	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	4
80.246.138.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.173.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.222.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.164	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
109.253.195.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
176.13.5.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.200.154	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.111.200.154	Block	2
188.120.150.222	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
2.54.131.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.200.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.129.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.185	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
176.13.18.126	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.74.83	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
87.68.58.1	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/bamahane	Block	1
5.255.88.68	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
83.28.187.210	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
80.246.136.132	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ***** , Observed *****	None	1
2.54.30.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	1
167.114.0.27	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/>israel	Block	1
37.237.184.25	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx adman	Block	1
212.25.102.57	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
2.95.34.113	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
109.253.222.38	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
66.249.74.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding)!{Fi}(&X-FO_PdXK/L0-[xh1YtKq1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
95.86.69.89	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1