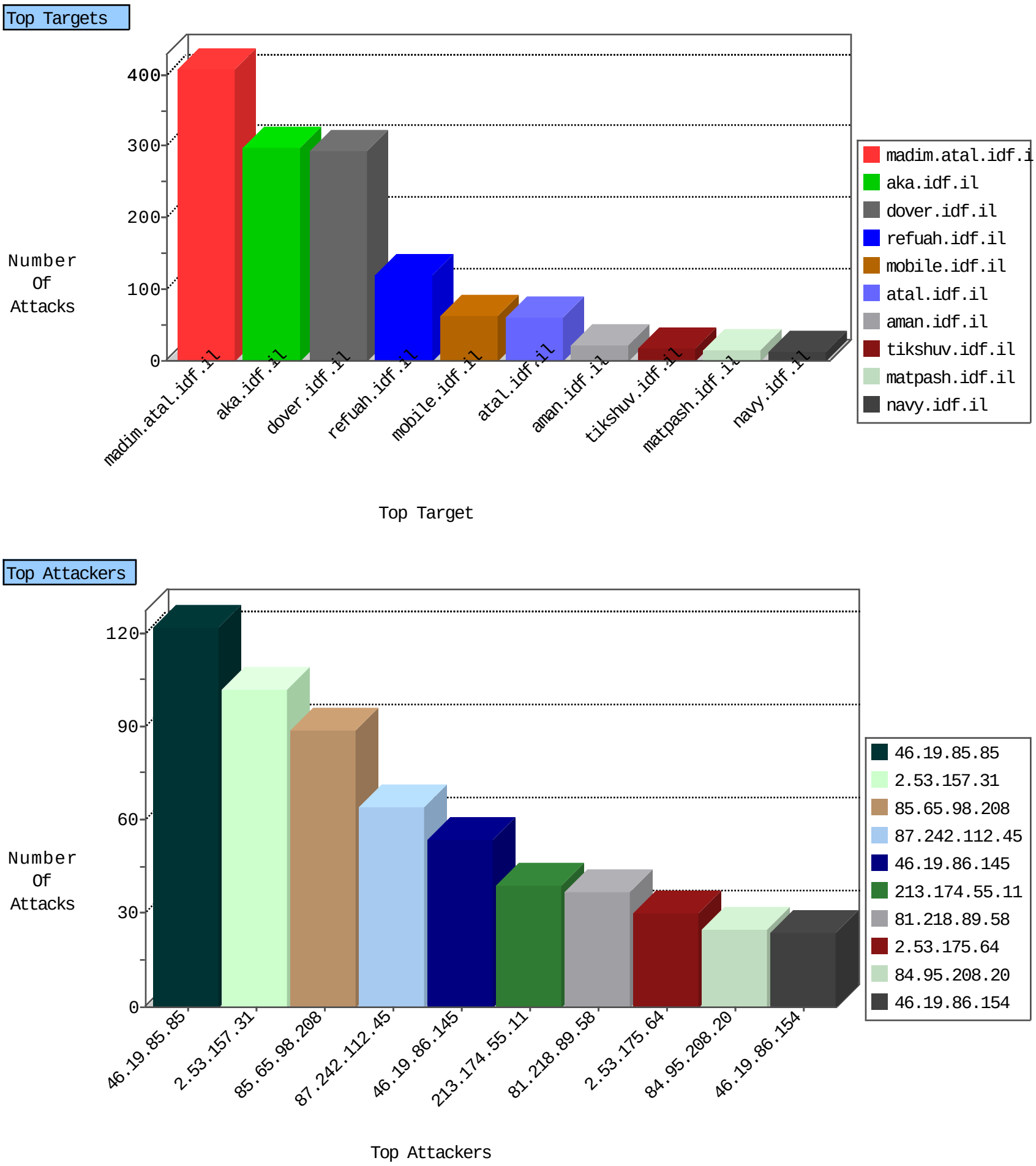
09-26-2016-10:04:05 to 09-26-2016-11:04:05

IDF Under Attack Daily Report



09-26-2016-10:04:05 to 09-26-2016-11:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
37.142.11.16	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
84.94.208.121	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.74.67	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
210.19.13.209	Malaysia	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
45.32.205.135	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

09-26-2016-10:04:05 to 09-26-2016-11:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.174.55.11	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
87.242.112.45	Russian Federation	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
50.63.196.229	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.242.112.45	Russian Federation	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
176.9.131.69	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
88.198.16.12	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
87.242.112.45	Russian Federation	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-26-2016-10:04:05 to 09-26-2016-11:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.242.112.45	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	46
213.174.55.11	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	27
50.63.196.229	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
2.55.129.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.174.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.21.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.238.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.176.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.159.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.132.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.8.46	Russian Federation	e.chinuch.idf.i	ET SCAN NMAP -sS window 1024	1
195.200.205.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.183.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.196.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.130.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.186.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.219.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.53.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.27.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.63.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.80.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.191.193	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
13.90.253.185	147.237.76.199	United States	e.nakchal.idf.i	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1

09-26-2016-10:04:05 to 09-26-2016-11:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.89.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
2.53.175.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
62.0.201.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
176.13.251.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	23
46.19.86.154	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
62.0.224.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
62.0.207.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
62.0.244.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.232.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.53.39.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.42	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.137	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
62.0.252.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.151.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
62.0.212.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.168.89.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.147.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.200.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.142.38	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.150.59	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
194.90.209.235	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.89.106	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.86.154	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.39.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
156.204.25.7	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.114.168.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.94.208.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.39.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.164	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.101.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.154	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.240.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.192.53	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-26-2016-10:04:05 to 09-26-2016-11:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
2.53.157.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
85.65.98.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
176.13.14.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
37.26.148.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.210.165.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
10.30.10.166	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan	Block	6
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.115.171	Block	5
176.13.16.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.53.26.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.72.138.1	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
176.13.23.144	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
81.218.173.237	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$txtSearch in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method	Block	1
81.218.37.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/scrollstrech.gif	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/m/english/	Block	1
212.117.137.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
82.80.193.240	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.142.10.48	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Unknown HTTP Request Method <tµþÃ‹J[[#1]]èjýyMÂakú;[[#1]]•dÃ‡'[[#30]]âv~v[[#8]] in URL	Block	1
68.180.228.174	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
2.55.18.73	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.27	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/haredim/general.aspx	None	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 3c05yigxk14z1ycyfnrk255 in URL	Block	1
180.76.15.158	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	NULL Character in Method	Block	1
81.218.89.58	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.73.130	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
2.53.30.169	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1085-he/refuah.aspx	Block	1
139.162.13.205	Singapore	147.237.0.15	kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
212.199.154.194	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 212.199.154.194	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.94.152.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8845-he'navy.aspx	Block	1
176.13.8.242	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
80.246.130.201	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
5.29.242.220	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
157.55.39.135	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
109.64.89.165	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 109.64.89.165	Block	1
66.249.66.203	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/mobile/	Block	1
193.128.33.248	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1

09-26-2016-10:04:05 to 09-26-2016-11:04:05