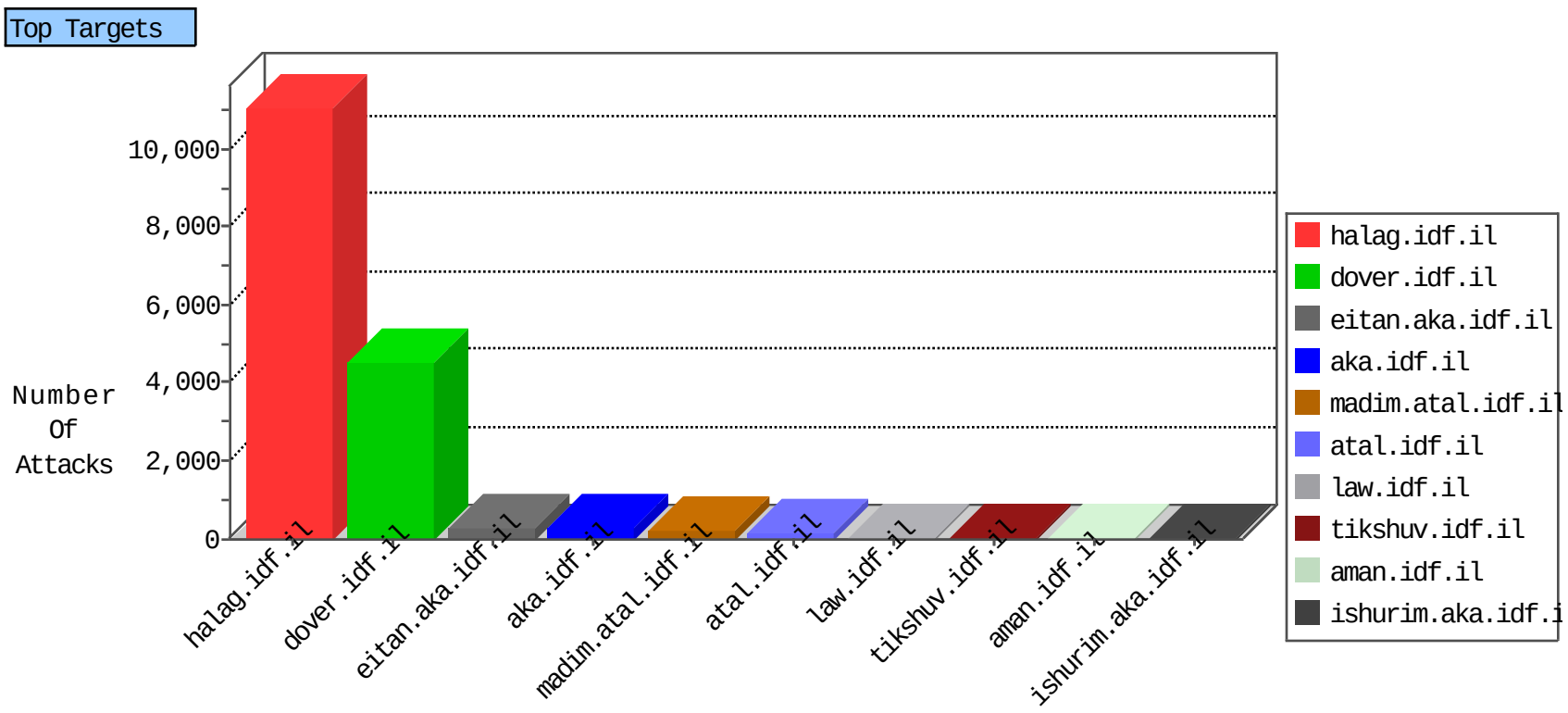
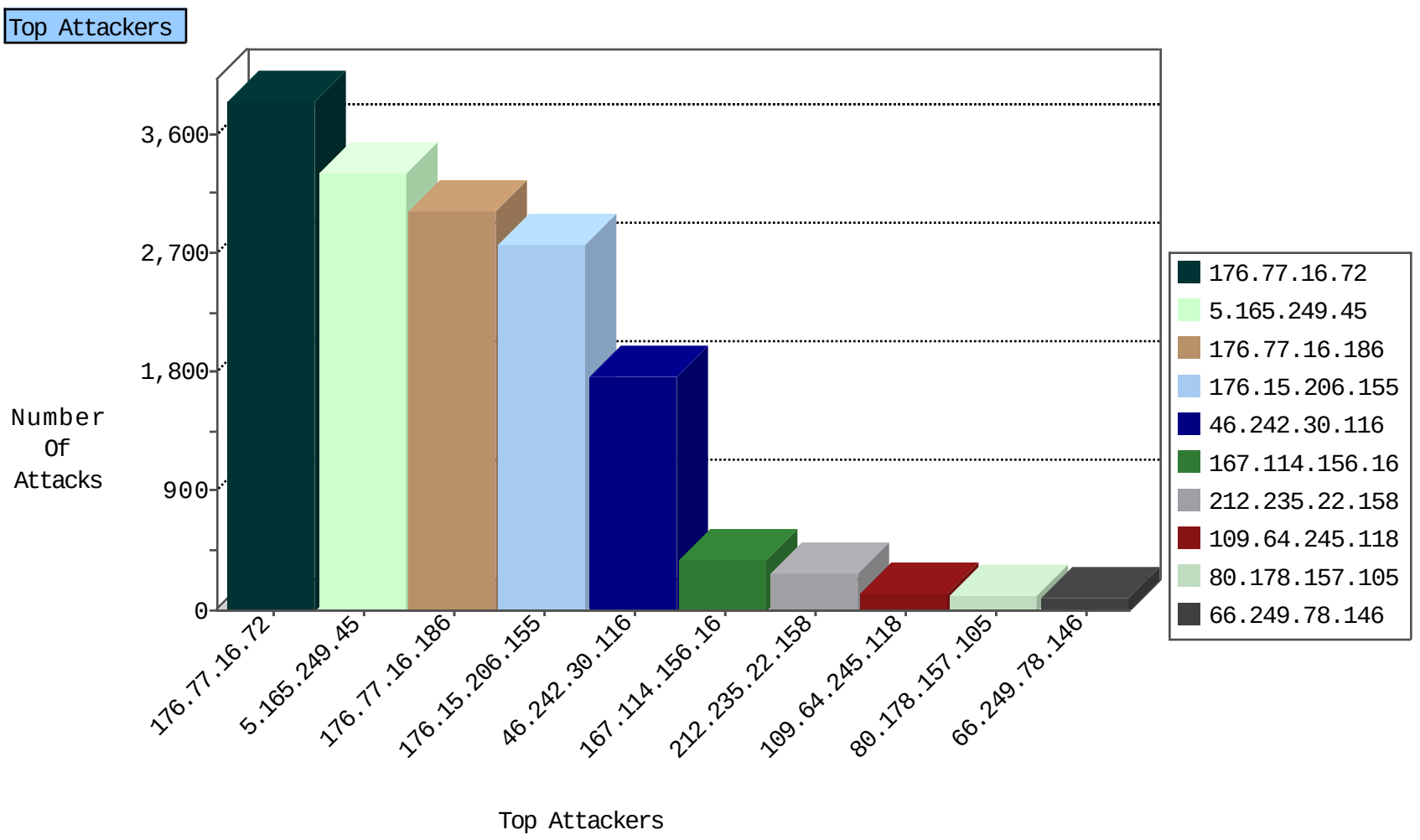
04-26-2016-14:04:02 to 04-26-2016-15:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-26-2016-14:04:02 to 04-26-2016-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	16161
176.77.16.186	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10021
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8433
176.15.206.155	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4094
46.120.78.166	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	106
5.165.249.45	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.77.16.72	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
109.65.106.217	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
46.242.30.116	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
153.226.48.48	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.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
87.69.136.46	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1

04-26-2016-14:04:02 to 04-26-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-14:04:02 to 04-26-2016-15:04:02

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
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
153.215.77.102	147.237.77.74	Japan	law.idf.il	Tehila - Perl LWP with fake user agent	2
81.169.171.4	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.38	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.122.143	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
197.45.132.217	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.122.143	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
184.80.10.136	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
119.92.55.24	147.237.76.34	Philippines	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.117.208.243	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
81.169.171.4	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
78.47.94.7	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.240.213.93	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.122.143	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
5.22.130.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
184.80.10.136	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 3072	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.43.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-26-2016-14:04:02 to 04-26-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.77.16.72	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	3654
176.77.16.186	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	2052
5.165.249.45	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	2027
176.15.206.155	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	1720
46.242.30.116	Russian Federation	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	1563
5.165.249.45	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1270
176.15.206.155	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1040
176.77.16.186	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	952
212.235.22.158	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	282
46.242.30.116	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	201
176.77.16.72	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	190
109.64.245.118	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	129
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
37.26.146.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
77.87.228.68	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
62.210.181.90	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
176.77.55.154	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	38
81.218.165.241	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.53.42.87	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.32.179.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
87.69.202.26	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.240.197.234	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.150.150	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.77.16.186	Russian Federation	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.1.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.77.16.72	Russian Federation	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
54.240.197.233	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.165.249.45	Russian Federation	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.242.30.116	Russian Federation	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.120.197	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
207.241.231.201	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
5.102.242.216	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.39.194	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
141.0.13.3	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.199.174.254	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.157.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
80.246.136.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.53.23.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
5.22.134.217	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 5.22.134.217	Block	4
37.26.146.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.201.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.158	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
149.78.223.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.113.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.134.217	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	3
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.189.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
41.250.126.93	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
81.218.180.44	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
54.67.99.176	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
94.230.85.231	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
79.180.103.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
54.194.11.113	Ireland	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Malformed URL __atuvc=1	Block	1
84.228.0.150	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2413.jpg	Block	1
54.186.68.225	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
199.30.25.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.85.231	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20624-he/dover.aspx	Block	1
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method mv0omeq5oubmqll3cva; in URL __atuvc=1	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/70454.pdf	Block	1
54.186.68.225	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
202.139.196.105	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.245.118	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
157.55.39.154	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
52.221.225.3	Singapore	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
85.130.222.103	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.79.83	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/602-2265-he/patzar.aspx - paragraph_12	Block	1
54.186.68.225	United States	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
207.46.13.39	United States	147.237.76.86	navy.idf.il	Parameter Type Violation catId in www.navy.idf.il/navy/watercrafts.aspx	Block	1
109.65.188.252	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
66.249.66.99	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3493.jpg	Block	1
54.67.99.176	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.19.249	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
54.186.68.225	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/wp-login.php	Block	1
109.253.150.249	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version __atuvs=571f55bc6e05e89f000	Block	1
2.53.12.5	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.108.103.14	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1