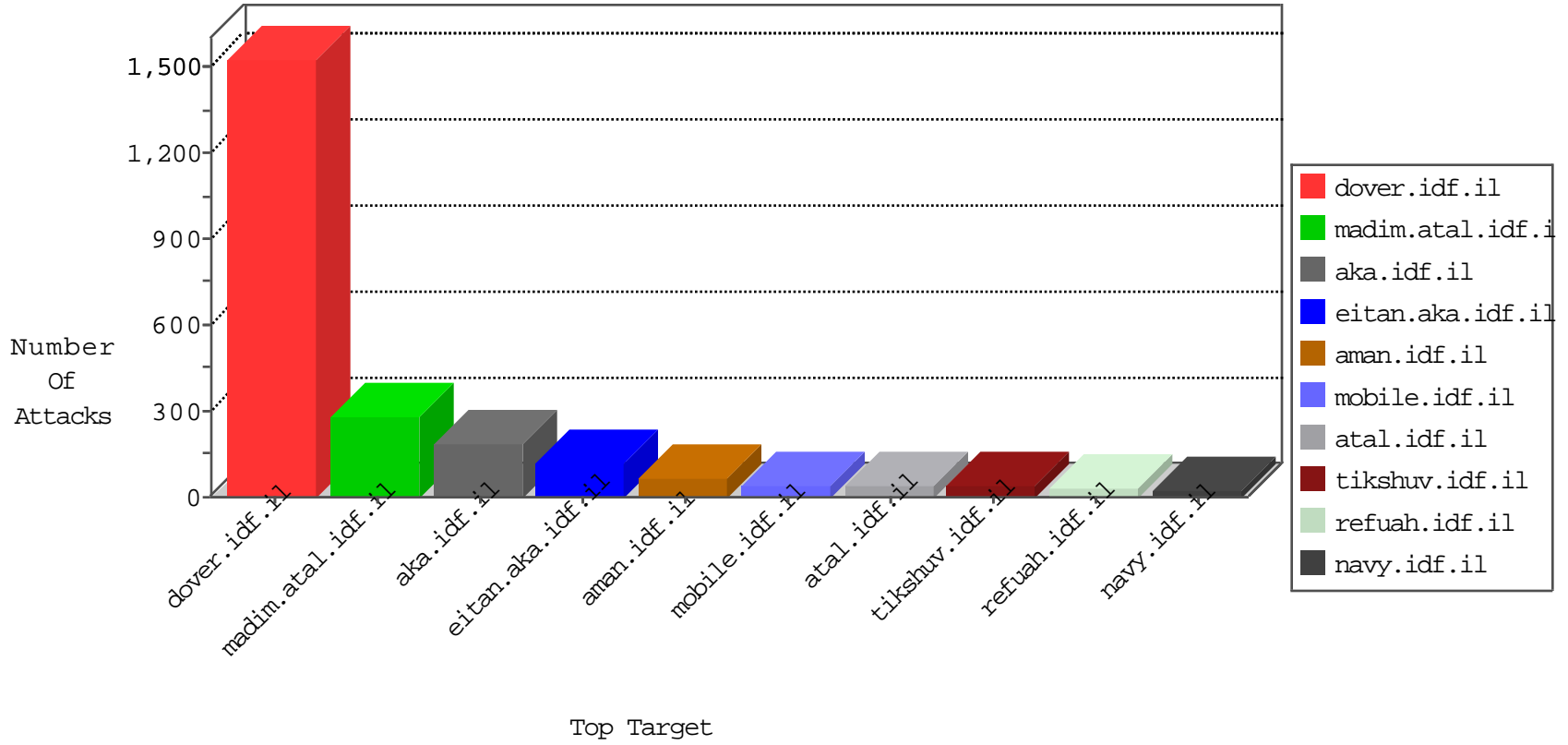


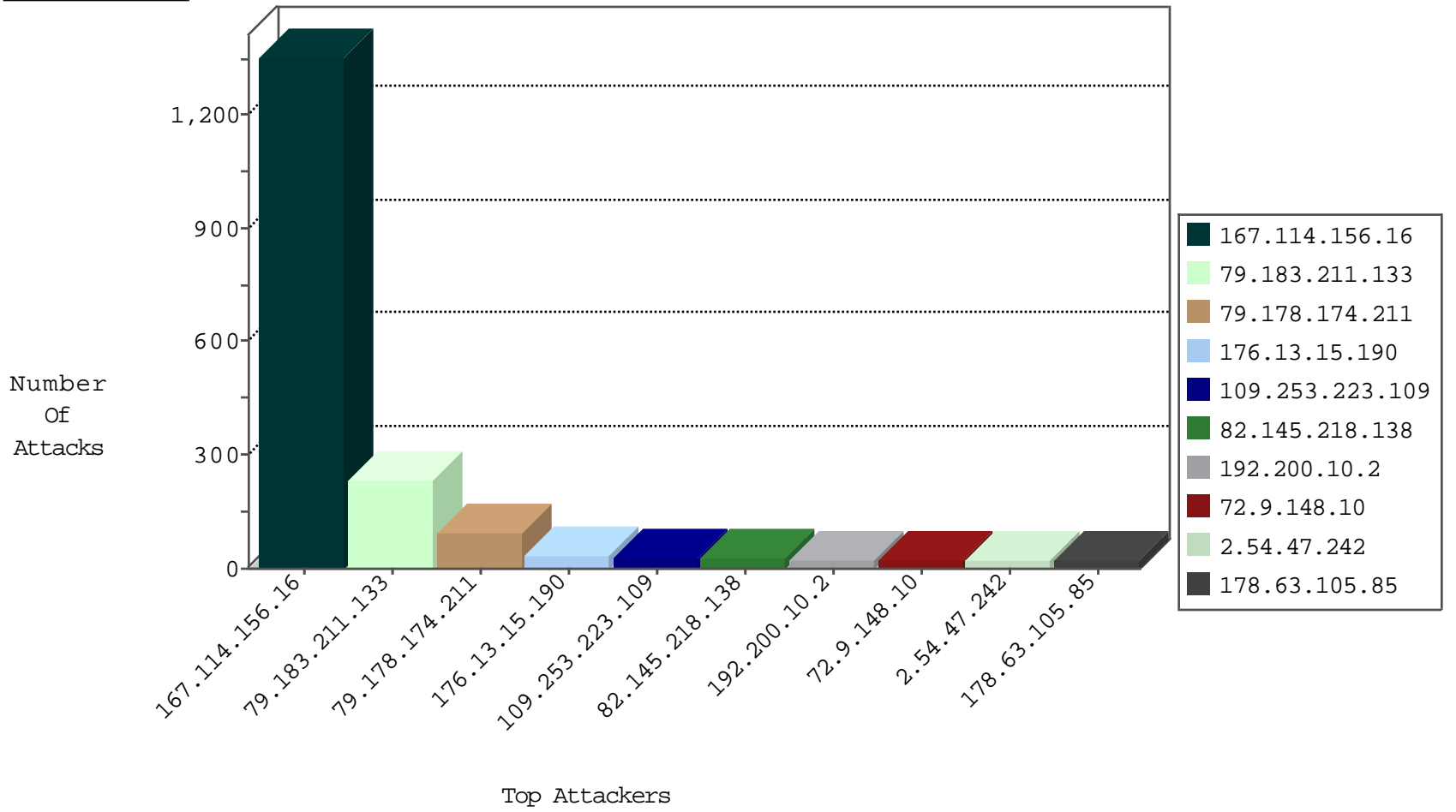
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3997
82.145.218.138	Europe	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	26
175.139.170.130	Malaysia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
82.145.210.188	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
12.7.121.130	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.187.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
109.160.151.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
85.130.129.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## 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	4
109.253.223.109	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
2.54.161.192	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
61.153.237.122	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	2
208.71.68.132	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
208.71.68.132	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
82.117.208.243	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.216.84.147	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.216.84.147	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
60.12.88.242	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	1
208.71.68.132	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
208.71.68.132	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.194	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.216.84.147	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.216.84.147	147.237.76.148	Taiwan	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.174.211	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
192.200.10.2		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
176.13.15.190	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
109.253.223.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
176.13.12.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.223.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
149.78.47.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.15.190	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
207.46.13.99	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.116.63.93	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	6
185.32.179.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.109.232	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.53.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.215	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.32.179.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.148.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.47.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.171.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
80.246.136.216	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
2.54.47.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
37.46.39.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.84	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.171.192	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.136.216	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	4
87.71.10.8	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.124	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
2.54.47.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.47.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
2.52.171.192	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
2.54.47.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.52.171.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.29	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.128	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.114.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.185.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.138.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.211.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	234
176.13.15.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.64.122.33	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.64.122.33	Block	5
109.64.122.33	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
52.90.128.17	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	4
149.78.236.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.47.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.246.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
197.113.138.144	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.113.138.144	Block	2
156.156.2.227	Tanzania, United Republic of	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.138.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.232.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.79	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/109843.pdf	Block	1
157.55.39.49	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
94.230.93.98	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.249.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
185.32.179.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
66.249.66.36	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
149.78.47.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.254.65.121	Romania	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.69.242.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.58.237	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
46.19.86.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
197.113.138.144	Algeria	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2297.jpg	Block	1
37.212.73.255	Belarus	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
87.71.10.8	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 87.71.10.8 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
180.76.15.161	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
85.65.49.191	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2828.jpg	Block	1
37.212.73.255	Belarus	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
87.71.10.8	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.25.148.240	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
46.121.79.81	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.186.37.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/5/size220x0/1655.bmp	Block	1
87.68.148.169	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
197.113.138.144	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/super-admin/	Block	1
79.178.174.211	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
46.19.85.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.11	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.82	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.179.41	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.25.148.240	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
87.69.224.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
207.46.13.95	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1