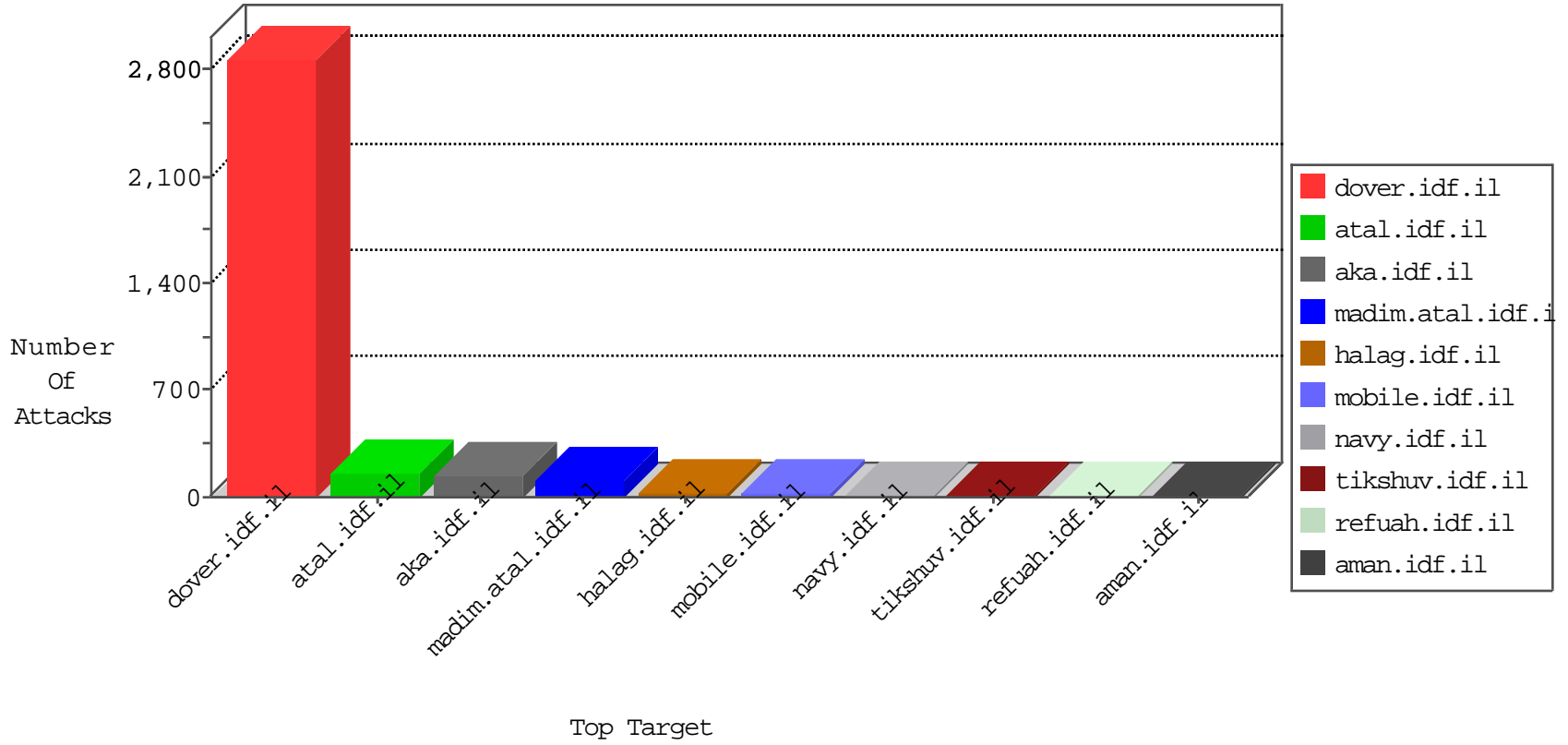


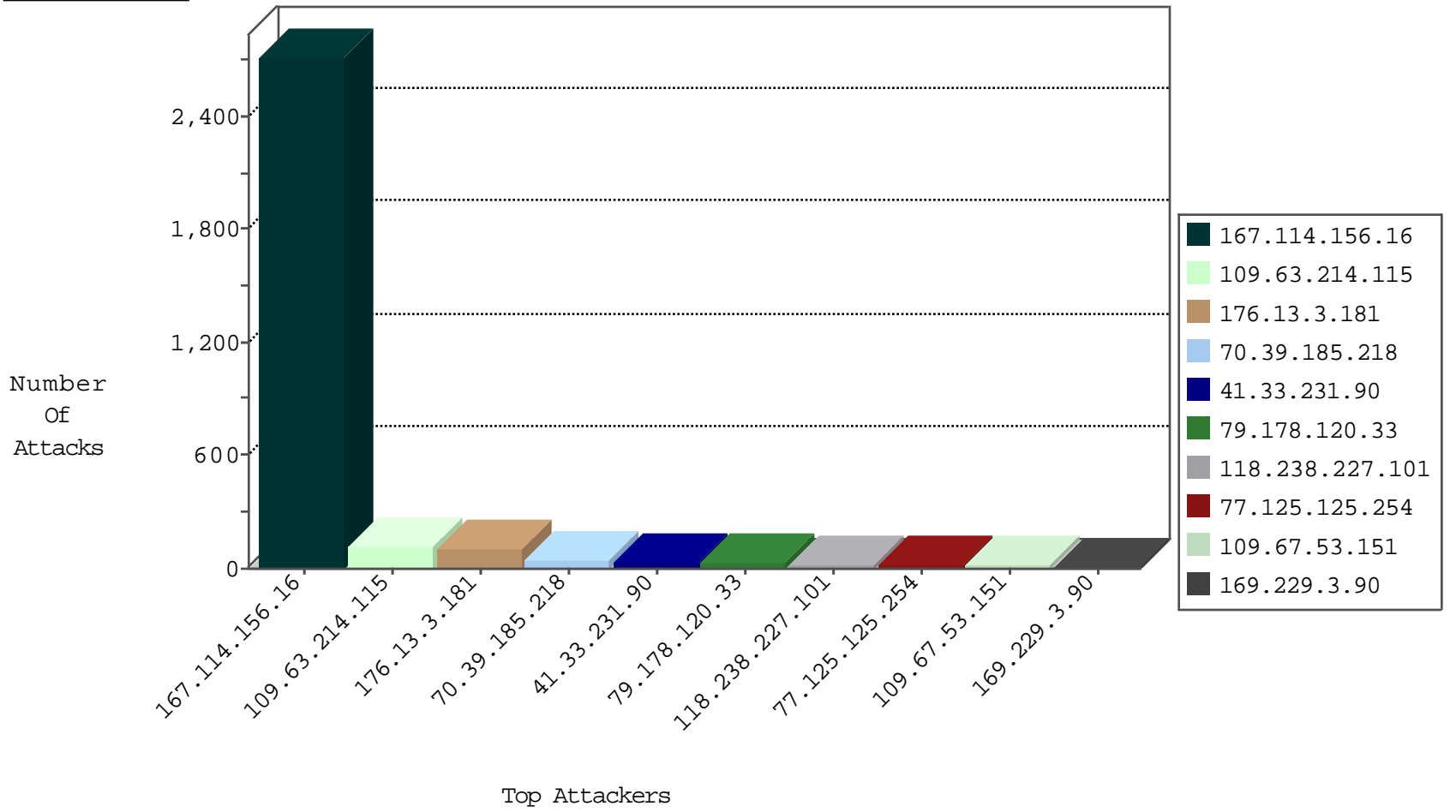
IDF Under Attack Daily Report



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	3367
70.39.185.218	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
109.63.214.115	Russian Federation	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	3
109.63.214.115	Russian Federation	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
70.39.185.218	Satellite Provider	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Https	drop	2
192.129.227.26	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
66.249.64.165	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
51.254.212.184	United Kingdom	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
192.129.227.26	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
51.254.212.184	United Kingdom	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

12-04-2015-17:04:01 to 12-04-2015-18:04:01

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.202	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.201	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
187.36.50.5	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
161.202.41.12	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
89.219.56.200	147.237.77.176	Estonia	matpash.idf.il	ET SCAN NMAP -f -sS	1
220.245.240.26	147.237.76.176	Australia	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.202	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
199.101.186.201	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
199.101.186.201	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
190.147.216.34	147.237.8.27	Colombia	e.medim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
187.36.50.5	147.237.0.15	Brazil	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.219.56.200	147.237.77.176	Estonia	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
220.245.240.26	147.237.76.176	Australia	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.63.214.115	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	105
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.178.120.33	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
118.238.227.101	Japan	147.237.77.233	atal.idf.il	drop	SAM rule	drop	24
70.39.185.218	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
70.39.185.218	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
77.125.125.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.57.131.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.142.250.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.254	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.53.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.67.53.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.133.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.159.103	Israel	147.237.72.156	anan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
141.0.15.66	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
100.127.229.117		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.132.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.13.3.181	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.30.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.157.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.120.33	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
31.210.178.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.192.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.176.34.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.110.39.144	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.186.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.178.79.155	Ukraine	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.211.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.15.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.103.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.164.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.117.224.177	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.142.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
176.13.7.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.139.61.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
169.229.3.90	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
176.228.175.19	Israel	147.237.76.147	chimuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
141.212.121.192	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
169.229.3.90	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
176.13.3.181	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.64	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
79.178.110.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
46.121.128.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
2.54.163.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
185.3.146.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.50.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.36.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.37.37.121	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
176.13.2.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.154.10.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.222.48.117	Finland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
207.46.13.126	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.aspx	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	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/6/3156.jpg	Block	1
109.160.177.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.128.78	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.128.78	Block	1
2.54.28.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.24.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.120.33	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.61	Block	1
37.26.149.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.37.37.121	Egypt	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3493.jpg	Block	1
141.212.122.64	United States	147.237.76.42	refuah.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
2.54.34.14	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.65.60.23	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
79.179.192.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.117	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/general/general.aspx	Block	1
66.249.67.214	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3142.jpg	Block	1
185.3.146.91	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
109.64.12.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
37.140.141.31	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.94.161.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.161.113	Block	1
2.52.17.247	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.52.17.247	Block	1
197.37.37.121	Egypt	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/geut/english/index.html>	Block	1
54.152.76.94	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/602-2215	Block	1
149.78.184.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.218.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/matpash/	Block	1
79.183.51.208	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
207.46.13.126	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.126	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1233-he/atal.aspx	Block	1
109.64.133.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1