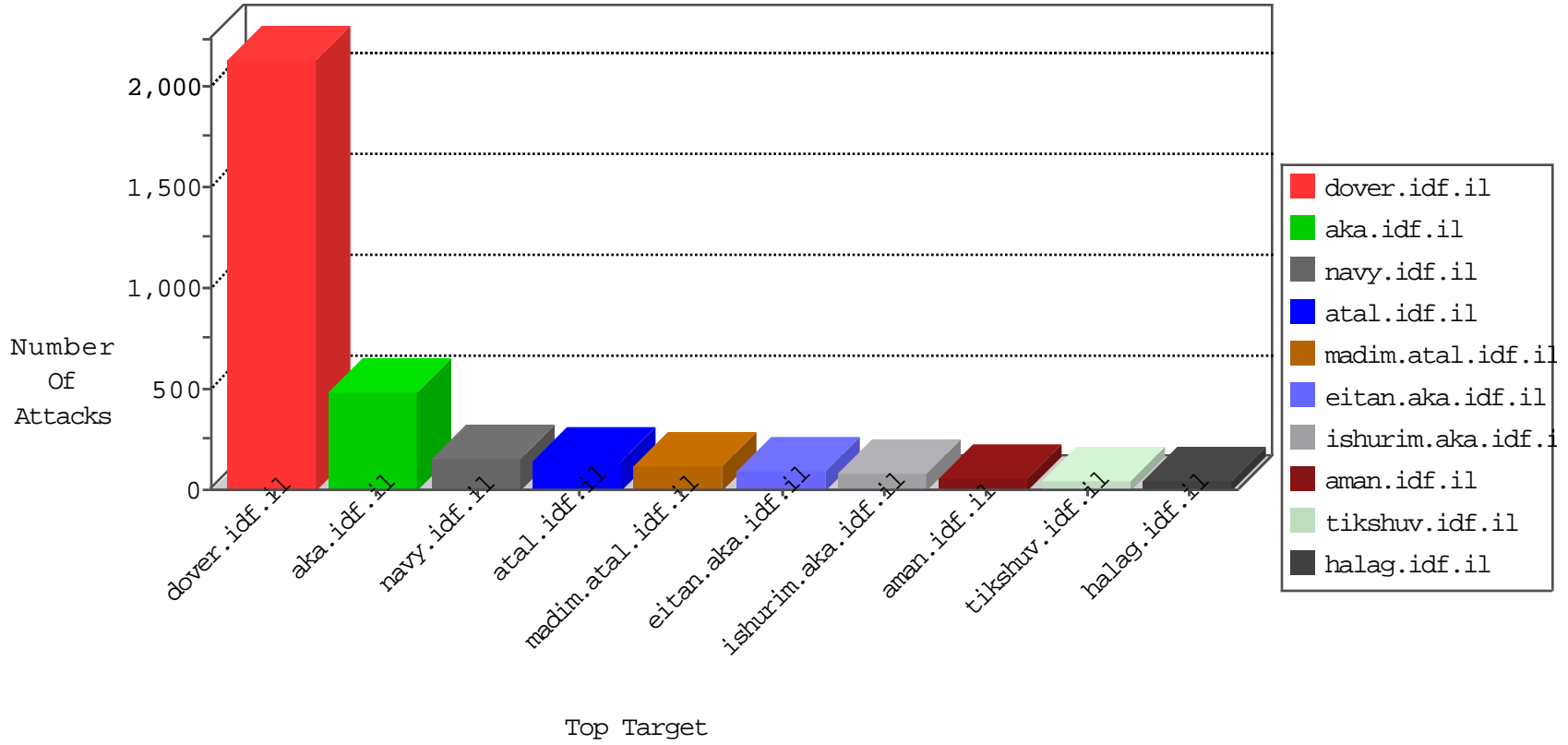


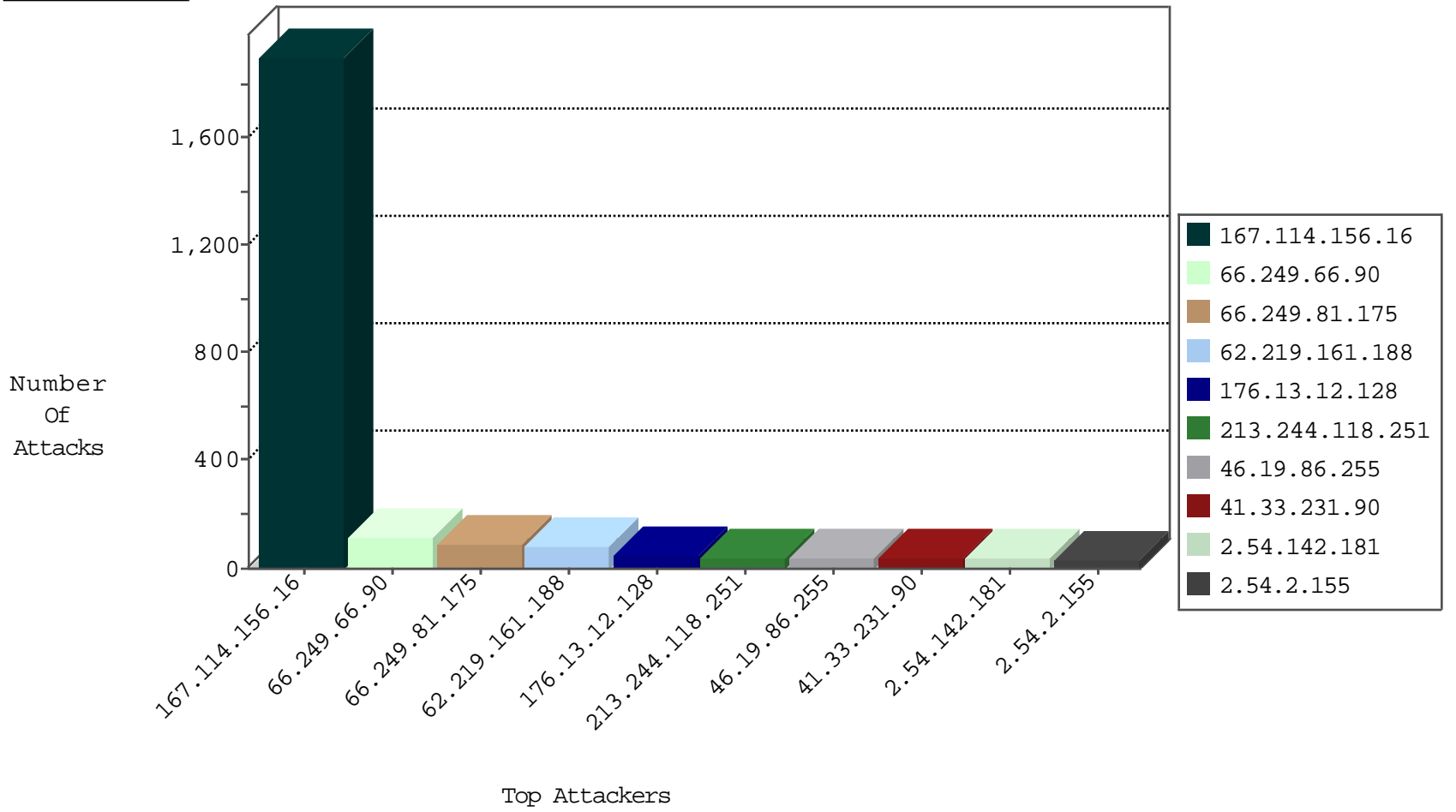
# IDF Under Attack Daily Report



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	3280
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	171
185.130.5.201		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
68.71.86.140	United States	147.237.76.197	e.himush.idf.il	JIM_Purple_Con_Limit_Http	drop	1
77.247.178.132	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.90	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	119
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
2.52.187.39	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
193.105.134.220	147.237.76.34	Sweden	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
173.199.74.136	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.19.86.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.158.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.37.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.199.74.136	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.149.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.130.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.150.94	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
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	90
62.219.161.188	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
46.19.86.255	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
2.52.40.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
213.244.119.245	Palestinian Territory Occupied	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.81.38.151	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.80.17.163	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
213.8.204.24	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	17
213.244.119.251	Palestinian Territory Occupied	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.42.206	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.252	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
213.244.118.251	Palestinian Territory Occupied	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.2.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.86.57	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
81.218.251.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.168.164.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
217.194.197.94	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
213.244.118.251	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.52.186.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.72.22	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
115.114.191.92	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.244.118.251	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
62.0.72.22	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
84.94.205.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.24	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.67.41.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.142.181	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.179.25.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.38.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.138.127	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.53.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.139.149.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.142.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.90.95.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.142.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.6.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.57	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
2.54.156.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.82.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
40.77.167.17	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.142.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.183.146.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.134.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
212.150.218.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.218.112	Block	3
217.132.131.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.222.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.192.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.66	Israel	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	2
176.13.1.102	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.158.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
176.13.23.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
173.252.115.84	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.80	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
2.54.186.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
2.52.4.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.141.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.56.186	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
37.26.146.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.64	United States	147.237.0.15	kosher-kravi.idf.il	Distributed Malformed URL	Block	1
79.179.4.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
213.151.44.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.43.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
50.62.161.217	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mod_shopping/public/price-history	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
81.218.70.243	Israel	147.237.72.166	aka.idf.il	Cookie Tampering on cookie wb48617274: Expected 971DB37F, Observed 7F6A4C06	None	1
37.142.190.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.115.85	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/7/3097.pdf	Block	1
212.150.218.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/g	Block	1
5.22.130.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
109.253.194.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.0.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.41.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
84.108.205.18	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
46.19.85.66	Israel	147.237.76.86	navy.idf.il	Multiple Abnormally Long Request from 46.19.85.66	Block	1
176.13.16.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1