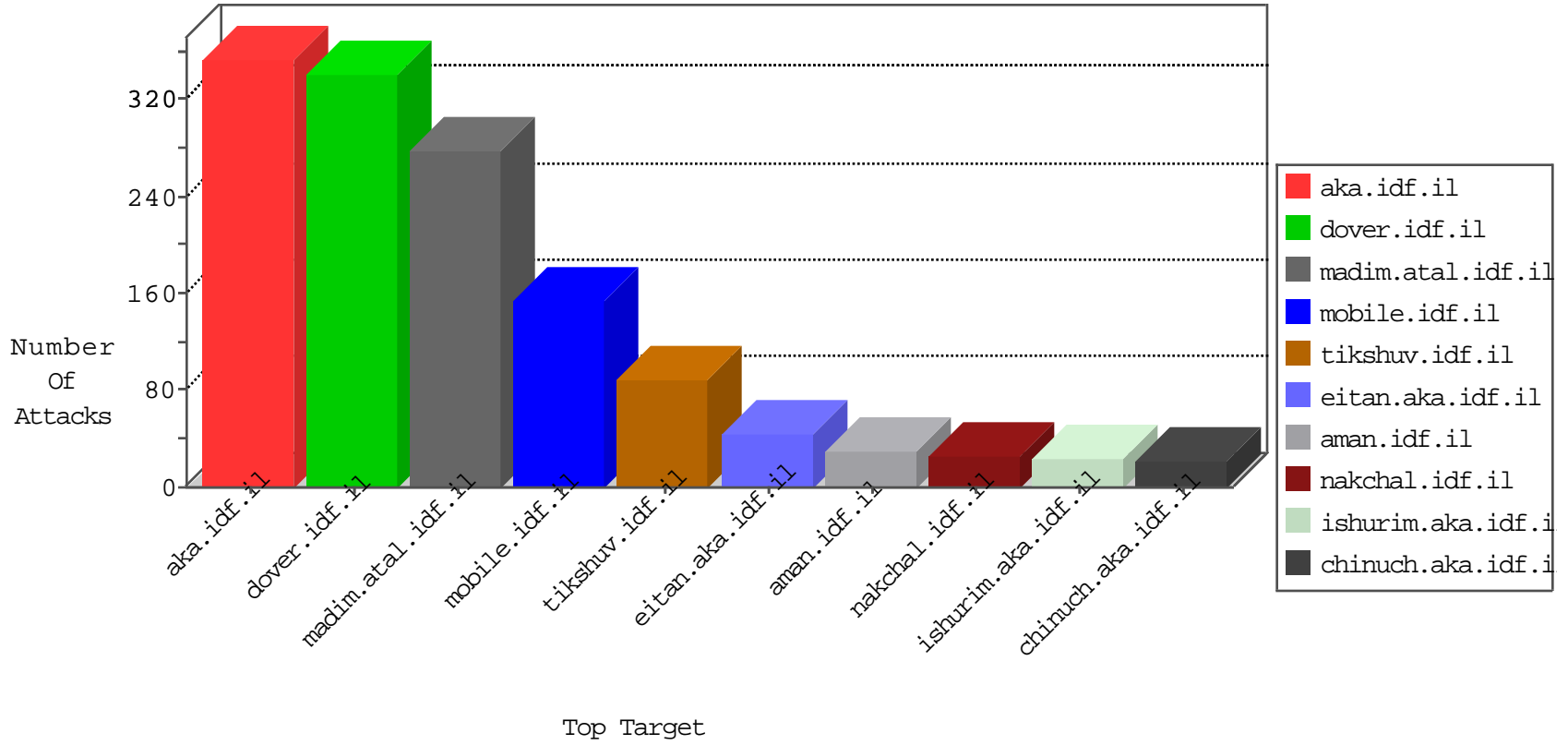


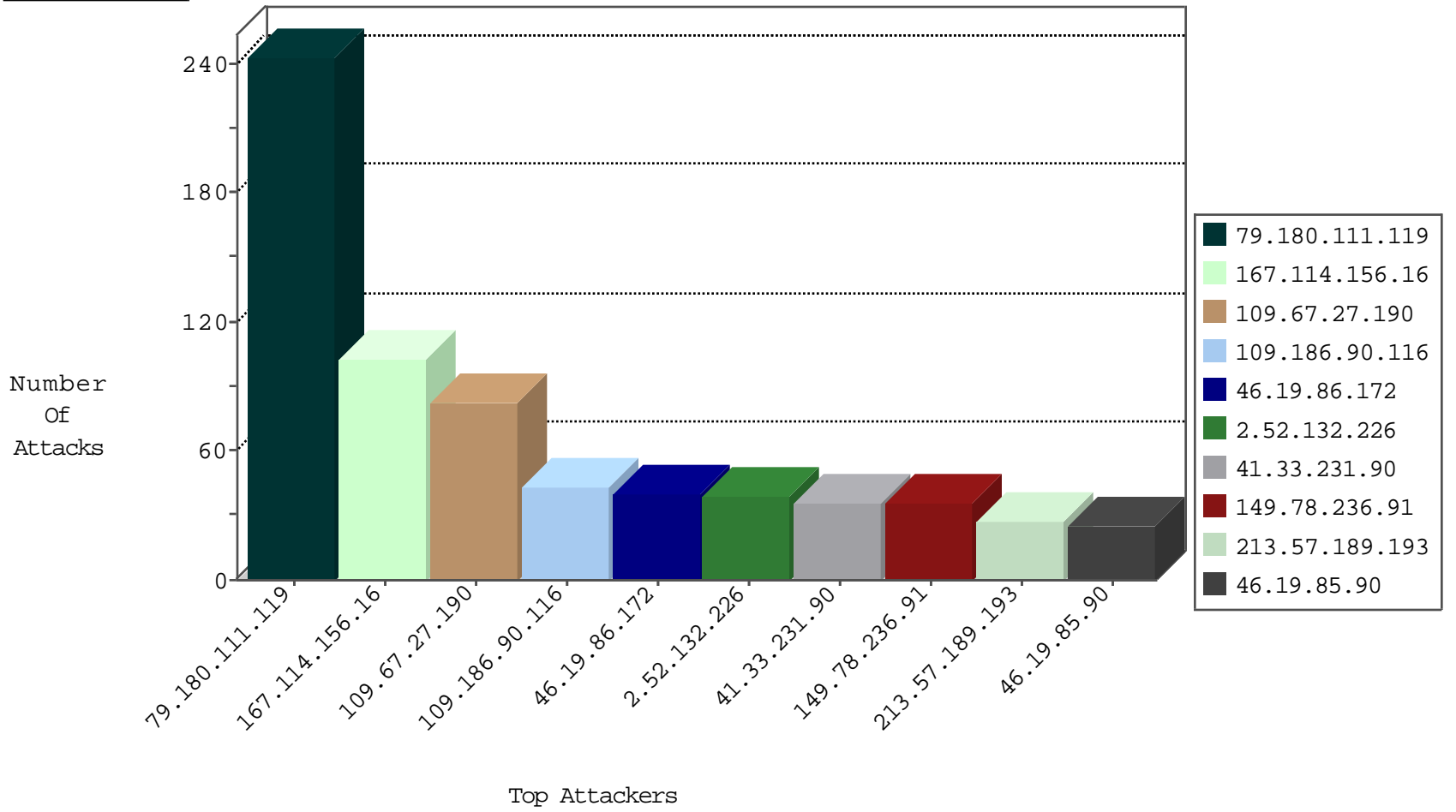
IDF Under Attack Daily Report



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	2896
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
52.33.66.29	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	5
94.102.56.238	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.236.91	Israel	147.237.72.166	aka.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	6
94.23.98.252	France	147.237.77.74	law.idf.il	4807: HTTP: PHP File Include Exploit	Block	4

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
94.23.98.252	147.237.77.74	France	law.idf.il	Tehila - Perl LWP with fake user agent	2
125.26.29.22	147.237.76.31	Thailand	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.68.29.67	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.28.219	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
151.217.178.88	147.237.77.235		sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
12.139.41.189	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.80	147.237.76.202		e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.72.156		aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.202.248.121	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
118.68.29.67	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
117.25.155.164	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
107.193.253.8	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
60.217.72.16	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.80	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.55	147.237.8.45		e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.186.90.116	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.57.189.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
149.78.236.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.236	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
79.177.160.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.57.134.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.52.132.226	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
31.168.149.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
109.66.6.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.117.207.221	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
109.65.181.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.89.217.227		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.66.100.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.180.109.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.193.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.254.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.188.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.117.157.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.218.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.50.71.105	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.183.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.193.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.183.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.239.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.69.249.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.52.19.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.134.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.132.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.64.34.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.54.48.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.229.49.69	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.209.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.116.130.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.128.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.29.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
188.29.164.128	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.132.226	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.111.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	186
109.67.27.190	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	82
79.180.111.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
192.116.130.156	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 192.116.130.156	Block	13
79.176.113.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
217.132.114.134	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	10
46.19.86.172	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
109.186.90.116	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	7
149.78.236.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
46.19.85.34	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
149.78.236.91	Israel	147.237.72.166	aka.idf.il	Unauthorized Method PROPFIND for www.aka.idf.il/sip_storage/files/9/59679.gif	Block	6
79.180.174.169	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.65.63.87	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
176.13.22.15	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.149.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.130.156	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
2.54.183.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.50.71.105	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.102.254.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.109.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.3.146.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.104.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.160.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
217.110.90.60	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.110.90.60	Block	2
176.12.139.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.218.144	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
109.65.181.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
37.26.149.214	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
157.55.39.179	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.65.19.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.154.145.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.23.98.252	France	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
213.151.48.214	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/&sa=u&ved=0ahukewikjty94hkahucvbokhvkucqagfggimaa&sig2=hcpkib19d30phmngbd2cg&usg=afqjcnhzd1g7cg-cebypxuyqfwh6yeg7q	Block	2
109.160.204.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.185.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.210.187.61	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 31.210.187.61 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 107.178.194.87	Block	1
217.110.90.60	Germany	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/giyus/general.aspx	None	1
79.177.120.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ the idf official website	Block	1
157.55.39.166	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/gen_204	Block	1
87.69.48.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
37.142.64.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.214.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
80.246.139.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	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