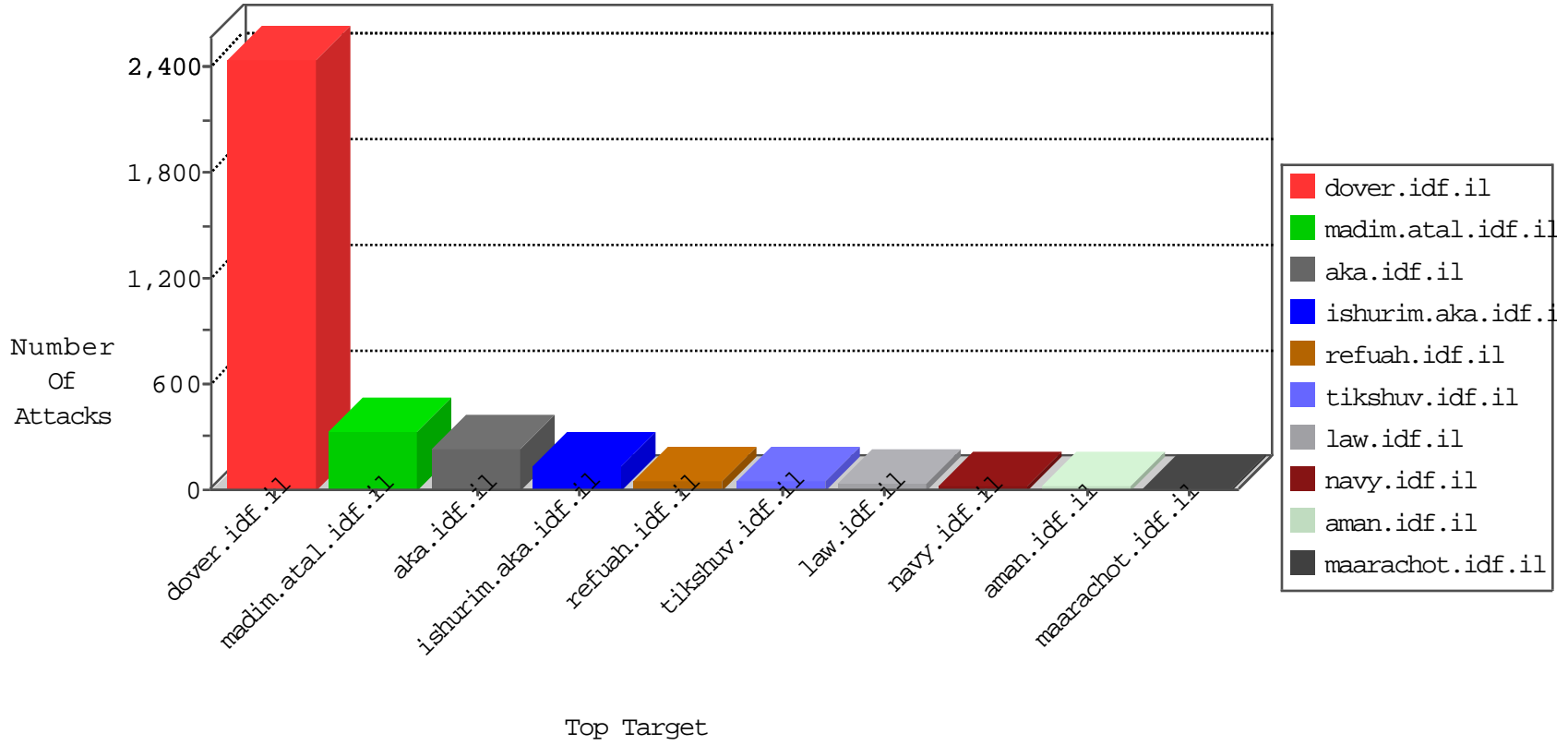


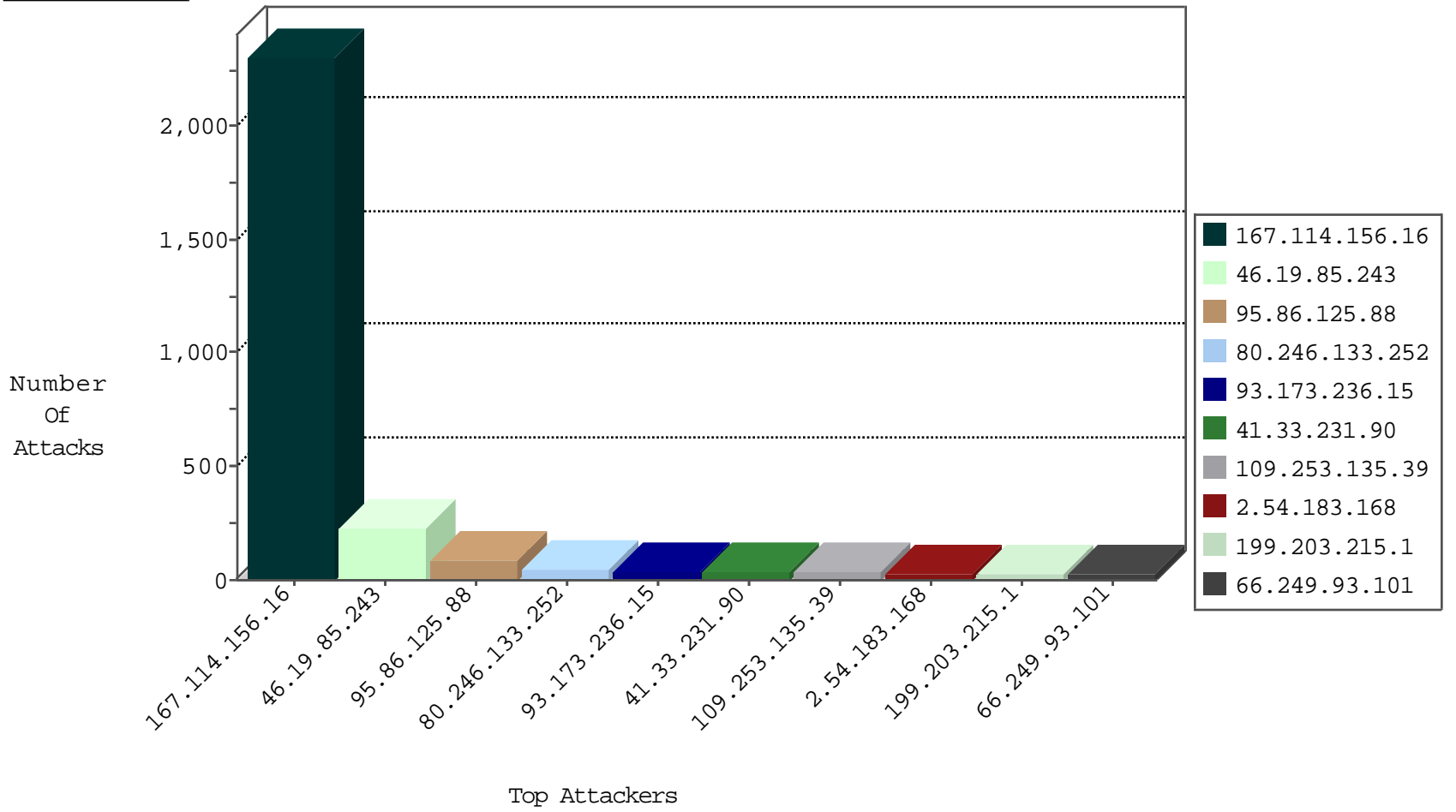
IDF Under Attack Daily Report



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	3036
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.66.160.66	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
142.54.169.166	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
104.233.70.144		147.237.76.198	e.yohanan.idf.il	Block_Udp_All_Nets	drop	1

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
66.249.93.101	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	28
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
93.157.85.152	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	1
88.204.187.90	147.237.77.226	Kazakstan	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
88.204.187.90	147.237.77.226	Kazakstan	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
80.246.136.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.157.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.113.195	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.226	Kazakstan	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
82.80.157.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
134.191.232.72	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
93.173.236.15	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
46.19.86.49	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.86.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
192.115.177.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
138.134.192.10	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
217.132.243.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.253.139.152	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.183.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
85.65.167.127	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.183.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.183.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.183.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.183.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.166.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.179.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.49	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.199.251.235	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.219.213.133	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.165.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.5.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.165.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.165.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.199.251.235	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.65.55.165	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.165.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.165.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.166.61	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
212.143.220.222	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.208.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.37.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.72.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
62.219.138.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.251.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.65.130.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.247.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	102
95.86.125.88	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 95.86.125.88	Block	84
80.246.133.252	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.133.252	Block	45
109.253.135.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.8.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.52.4.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
81.218.241.26	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	8
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.243	Block	7
85.64.115.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.128.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.158.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.54.157	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.64.182.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.211.34.236	Ukraine	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	2
109.253.219.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.228.112	United States	147.237.77.216	doover.idf.il	Parameter Type Violation pageNum in www.idf.il/1153-he/doover.aspx	Block	2
212.143.124.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	2
46.211.34.236	Ukraine	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.211.34.236	Block	2
62.210.180.192	France	147.237.77.216	doover.idf.il	Distributed eMail Hoarding	Block	1
213.152.161.40	Netherlands	147.237.77.216	doover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1
95.86.125.88	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many 404: Response Code per Session	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.23.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.158.105	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.81.250	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/layout.css	Block	1
212.76.104.239	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
87.68.78.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
176.13.7.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.140.160	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
77.75.77.17	Czech Republic	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/page/25/	Block	1
5.255.253.62	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.160.253.22	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
62.210.190.10	France	147.237.77.216	doover.idf.il	Distributed PHP Attempt	Block	1
213.152.161.40	Netherlands	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
84.19.190.106	Germany	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/doover.aspx.	Block	1
46.19.86.214	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
185.65.135.227	Sweden	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/doover.aspx.	Block	1
46.19.85.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.57.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.202.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.211.34.236	Ukraine	147.237.76.31	nakchal.idf.il	Multiple Admin Blocking from 46.211.34.236	Block	1
93.169.179.54	Romania	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
81.218.140.160	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1