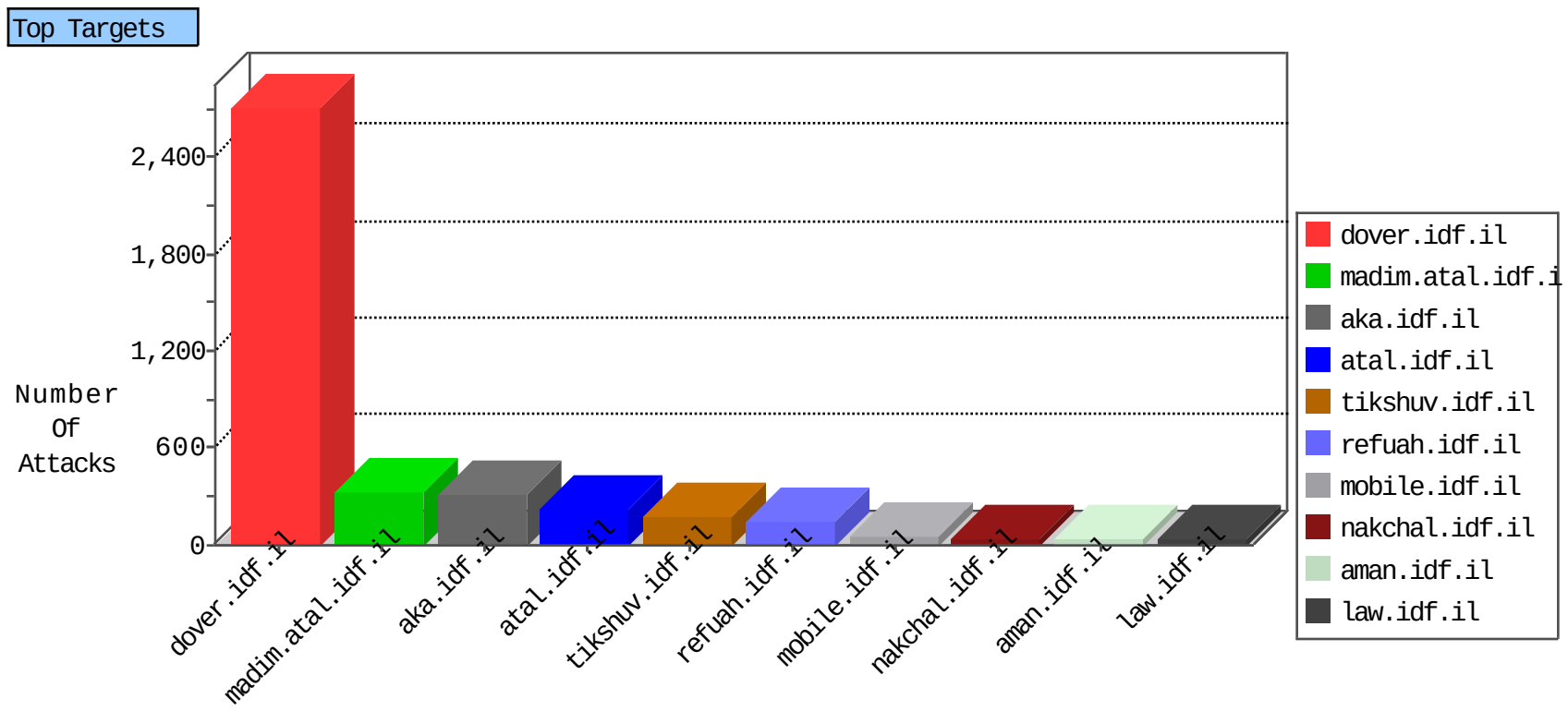
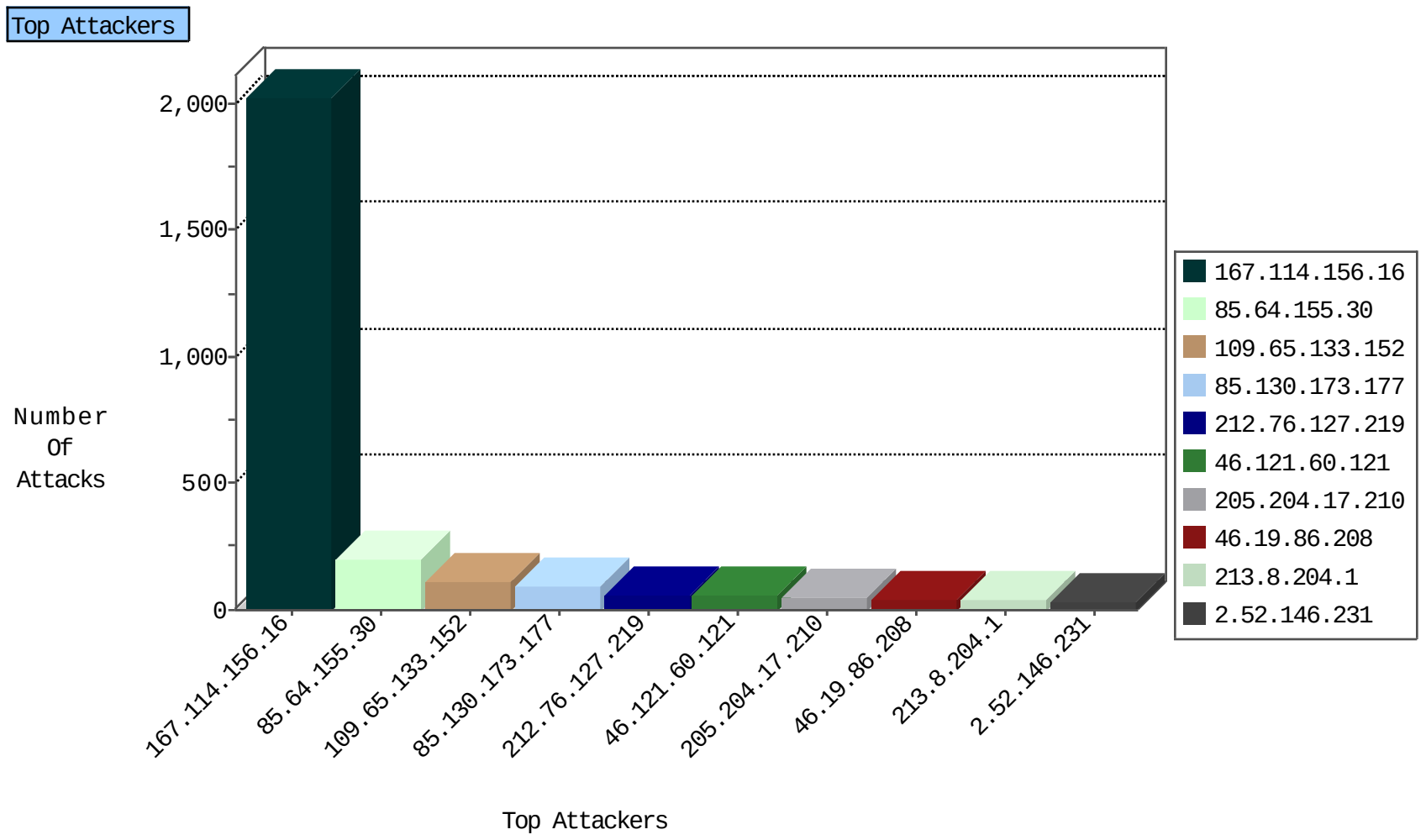
01-20-2016-19:04:08 to 01-20-2016-20:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-20-2016-19:04:08 to 01-20-2016-20:04:08

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	3038
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.67.201.245	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

01-20-2016-19:04:08 to 01-20-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.103	Italy	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-20-2016-19:04:08 to 01-20-2016-20:04:08

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
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
95.86.70.197	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
46.228.207.18	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
85.130.238.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.83.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.26.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.128.3.182	147.237.0.34	France	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.177.88.126	147.237.76.34	United States	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.76.86	Germany	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.13.88.58	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.1.105	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.254.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.71.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.82.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.146.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.212	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
212.117.154.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.13.88.58	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.53.217	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.1.105	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.72.166	Ukraine	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

01-20-2016-19:04:08 to 01-20-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	57
85.130.173.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
85.130.173.177	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
205.204.17.210	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
5.22.134.207	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
205.204.17.210	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
84.108.235.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
221.202.205.222	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
175.18.112.202	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
46.19.86.208	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.86.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
2.52.146.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
221.206.191.2	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
94.252.207.155	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
94.252.207.155	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
222.163.195.35	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
113.5.80.68	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
222.163.195.19	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
46.19.86.100	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
221.202.205.190	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
61.138.61.143	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.19.85.161	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.31.103.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.161	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
218.60.132.40	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
2.54.156.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
145.131.203.155	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
139.214.193.246	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
218.60.123.19	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.19.85.77	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
218.60.123.59	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
46.19.85.185	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.185	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.140	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.31.103.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.102	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.19.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.133.152	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.65.133.152	Block	111
85.64.155.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
85.64.155.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.155.30	Block	79
46.121.60.121	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
213.8.204.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
185.32.179.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.49	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	12
85.64.155.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 85.64.155.30	Block	11
213.8.204.76	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.76	Block	4
149.78.34.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.37.53	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
213.8.204.76	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
2.54.182.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.0.61	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.120.235.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.65	Block	2
89.139.243.252	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.179.105.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.168.200.244	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
149.78.252.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.61.129	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
46.120.20.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/mailbox.aspx/	Block	1
82.81.37.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.204.65	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
79.180.120.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.64.57.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
79.107.221.243	Greece	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
162.247.72.213	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
85.130.173.177	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.110.111.133	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
217.132.133.161	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/1.he/scroller/skin.css	Block	1
149.78.53.156	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
109.253.197.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/shared/usercontrols/headerupper/	Block	1
212.199.104.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.85	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
5.29.212.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.118.87	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
184.168.200.244	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/960.css	Block	1
149.86.191.95	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
149.78.53.156	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
84.94.164.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1