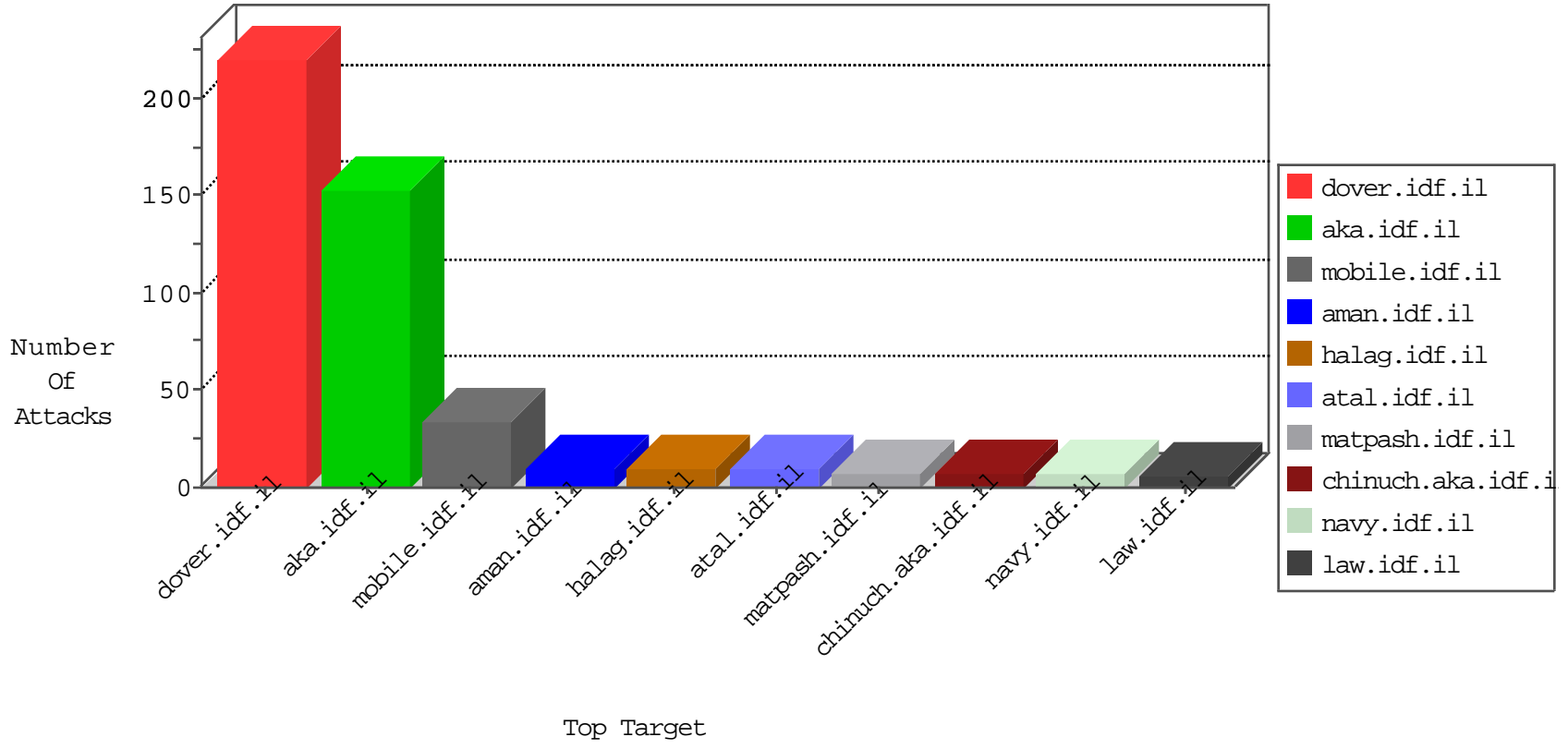


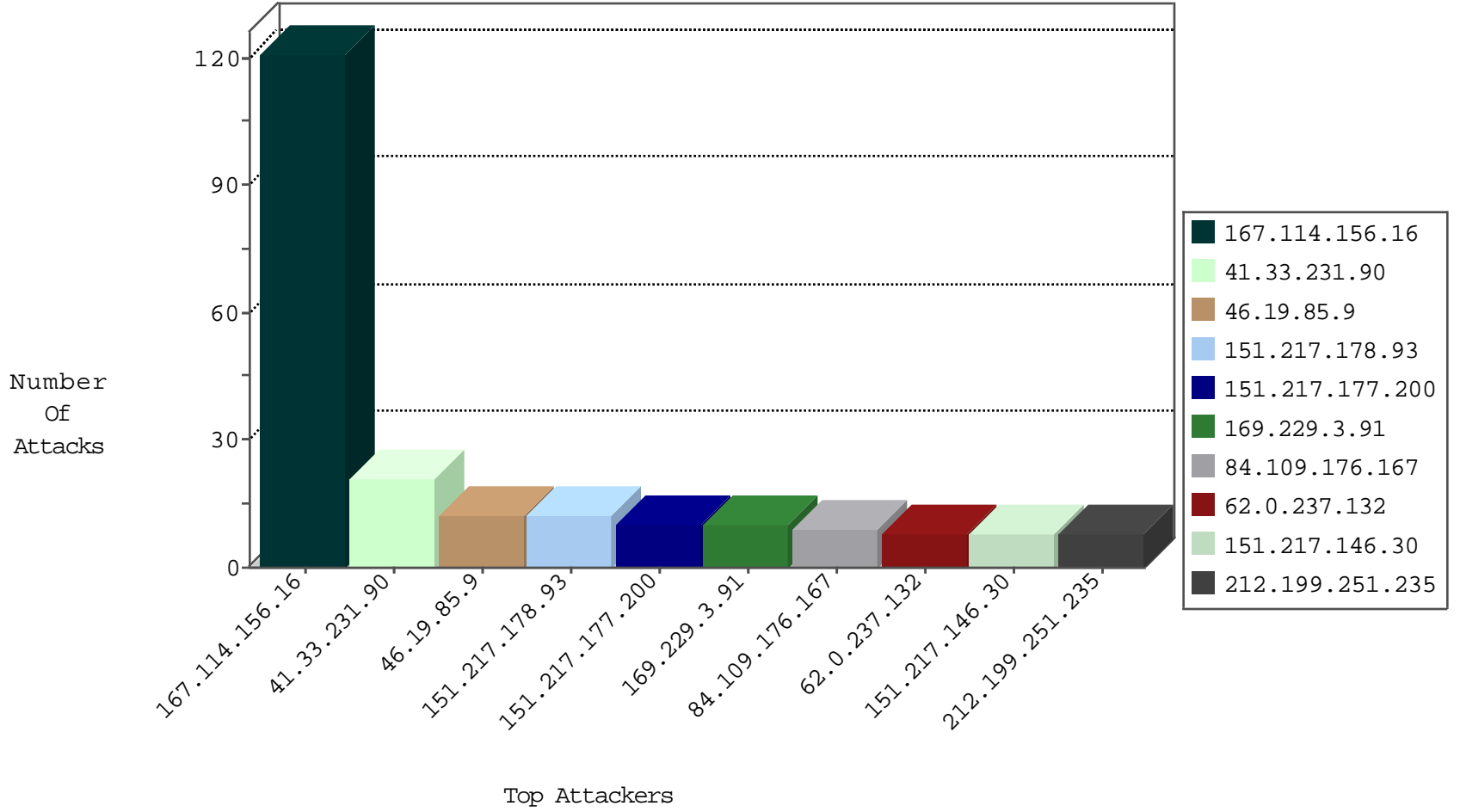
IDF Under Attack Daily Report



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	2568
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

12-30-2015-06:04:00 to 12-30-2015-07:04:00

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
73.169.61.25	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
88.204.187.90	147.237.77.121	Kazakstan	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.80	147.237.76.197		e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.80	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.135.139.53	147.237.77.216	France	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
190.249.184.162	147.237.76.30	Colombia	himush.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.177.200	147.237.77.234		halag.idf.il	SERVER-WEBAPP DELETE attempt	1
151.217.178.93	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.77.121		e.navy.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.93	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.93	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.93	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.93	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
95.86.106.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.93	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.178.143.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.80	147.237.76.34		yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.249.184.162	147.237.76.30	Colombia	himush.idf.il	ET SCAN NMAP -sS window 3072	1
151.217.178.55	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.93	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.77.212		e.dover.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.93	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.93	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.93	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
151.217.146.30	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.93	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.77.74	China	law.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	1
151.217.178.93	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
62.0.237.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.238.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
184.88.31.132	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
85.64.97.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.231.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.3.146.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.199.251.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.0.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.176.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
151.217.177.200		147.237.77.234	halag.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
212.199.251.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.109.176.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
82.81.18.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.5.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.197.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.180.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.94.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.176.195.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.168.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
84.109.176.167	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.8.42.177	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
80.246.139.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.29.72.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.25.233	United States	147.237.77.226	www.chamatz.aka.idf .il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
151.217.177.200		147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.168.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.43.103.24	Poland	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.46.39.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.121.229.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.166.74.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
217.132.106.176	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.8.42.177	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
132.73.81.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.25.233	United States	147.237.77.226	www.chamatz.aka.idf .il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
82.81.38.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
151.217.177.200		147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.72	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
14.145.255.126	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.60.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.13.21.253	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	4
5.29.101.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.19.85.152	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
84.111.71.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.181.162.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.10.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.198.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.160.150.67	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
149.78.84.162	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
66.249.66.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	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
109.65.207.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.19.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.172.166.23	United States	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/./style/shared/ie.css	Block	1
109.253.156.0	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
46.19.85.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
184.88.31.132	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
2.52.17.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.196.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
207.46.13.157	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sachar	Block	1
109.66.99.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.22.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.65.236.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.65.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
171.25.193.78	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2662.jpg	Block	1
198.135.0.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.52.132.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.15.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.176.167	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
151.217.177.200		147.237.77.234	halag.idf.il	Abnormally Long Request request version	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
89.138.180.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
37.142.64.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.76.15.30	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.119.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
174.59.187.72	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.253.200.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3141.jpg	Block	1