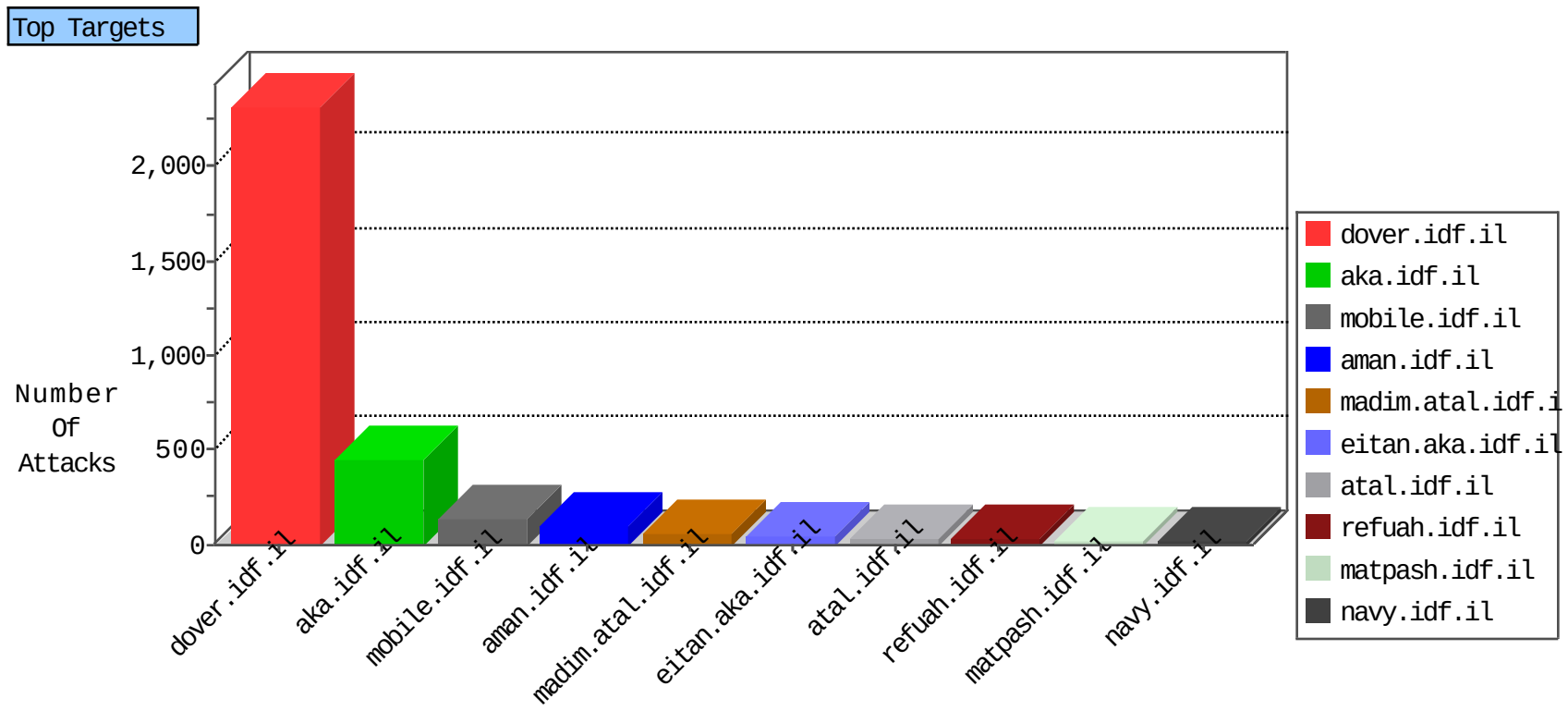
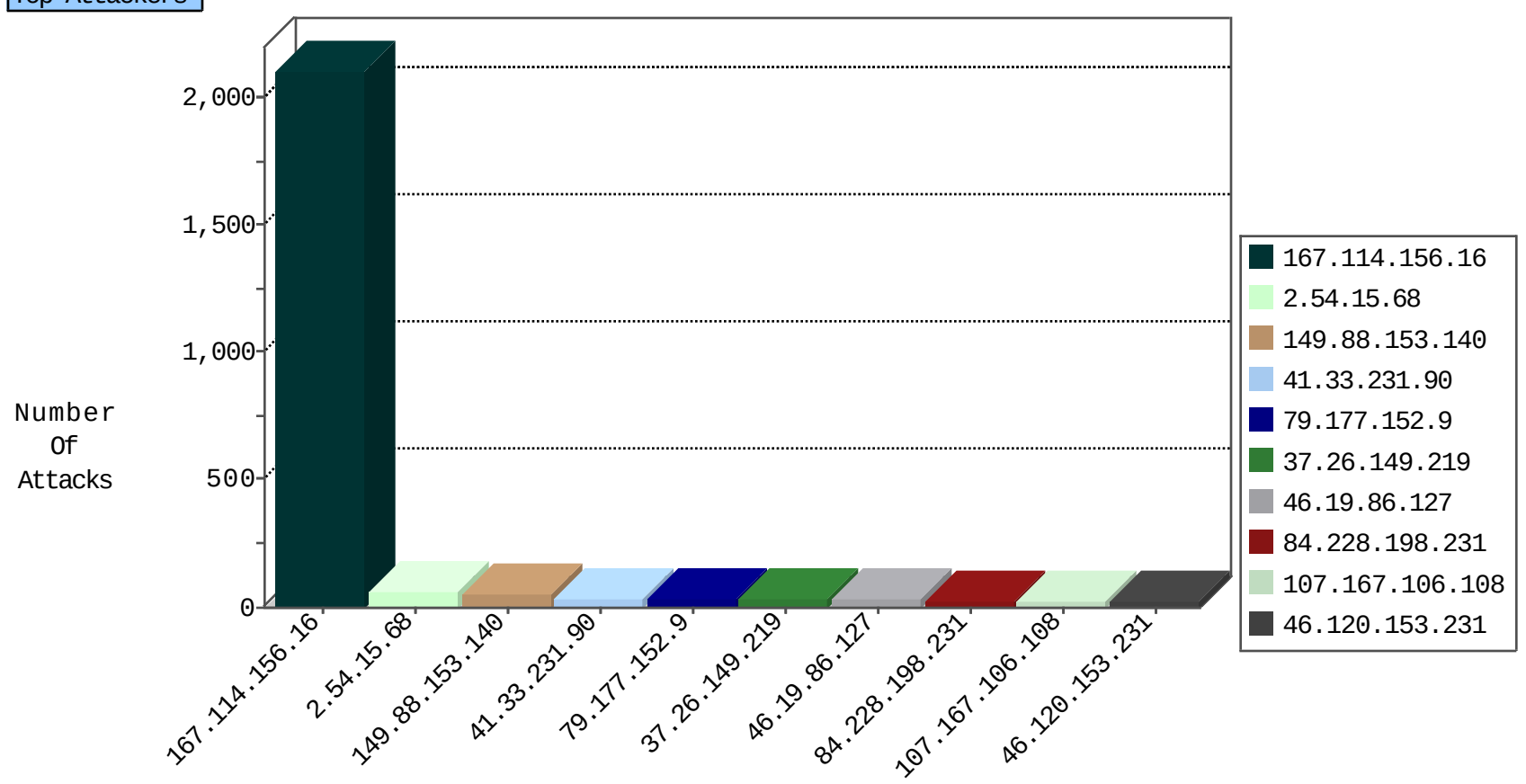
12-27-2015-19:04:02 to 12-27-2015-20:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-27-2015-19:04:02 to 12-27-2015-20:04:02

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	3202
118.96.205.3	Indonesia	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

12-27-2015-19:04:02 to 12-27-2015-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-27-2015-19:04:02 to 12-27-2015-20:04:02

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
66.102.8.243	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.160.225.135	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
151.217.26.35	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.23.96.131	147.237.76.30	Brazil	himush.idf.il	ET SCAN Potential SSH Scan	1
79.179.114.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.104.49.211	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
151.217.26.35	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.23.96.131	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
213.8.204.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.153.140	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
168.62.238.153	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
199.191.56.188	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.88	147.237.76.86		navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.235.254.181	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
151.217.26.35	147.237.77.243		mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
189.254.90.133	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
151.217.26.35	147.237.77.233		atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.159	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.82.106.200	147.237.76.202	India	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.26.35	147.237.77.176		matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.23.96.131	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
87.69.109.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.26.35	147.237.76.201		e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.23.96.131	147.237.76.38	Brazil	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
81.101.206.244	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.26.35	147.237.72.166		aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.23.96.131	147.237.0.200	Brazil	m4u.idf.il	ET SCAN Potential SSH Scan	1
218.104.49.211	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
151.217.26.35	147.237.0.33		idf.il	ET SCAN Potential VNC Scan 5900-5920	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
177.23.96.131	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.116.177.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.88	147.237.76.177		ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.235.254.181	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.188	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.63.152	147.237.77.179		e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.160.225.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
189.254.90.133	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.26.35	147.237.77.235		sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.173.160.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.202	India	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
151.217.26.35	147.237.77.179		e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.159	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.82.106.200	147.237.76.202	India	e.halag.idf.il	ET SCAN NMAP -f -sS	1
151.217.26.35	147.237.77.170		maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.23.96.131	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

12-27-2015-19:04:02 to 12-27-2015-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.15.68	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.219	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
84.228.198.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
107.167.106.108	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
79.180.162.39	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
79.182.132.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.13.9.223	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
37.26.147.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.183.19.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.186.90.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.120.125.43		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
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
80.178.97.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.18.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.228.234.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.171.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.20.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.85.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.173.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.50.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.32.179.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.26.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.50.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.111		147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
213.57.129.223	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.15.68	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
213.57.129.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.181.178.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.145.117	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.15.68	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
89.139.146.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.15.68	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.153.231	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
31.168.100.81	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.253.197.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.187.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.117	Israel	147.237.72.166	aka.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
37.26.147.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

12-27-2015-19:04:02 to 12-27-2015-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.152.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.120.153.231	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.153.231	Block	18
46.19.86.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 149.88.153.140	Block	6
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 149.88.153.140	Block	4
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 149.88.153.140	Block	4
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 149.88.153.140	Block	4
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 149.88.153.140	Block	4
46.19.85.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.179.202.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.202.24	Block	3
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 149.88.153.140	Block	3
176.13.15.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.6.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.38.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.219	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	2
85.250.73.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.186.163.32	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.253.157.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.162	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
46.19.86.156	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 149.88.153.140	Block	2
87.68.248.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.125.43		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.44.140.55	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 31.44.140.55	Block	2
109.64.150.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.176.53.105	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/haredim/general.aspx	Block	2
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 149.88.153.140	Block	2
109.67.99.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 149.88.153.140	Block	2
95.35.199.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.22.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.52.175	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
31.13.102.109	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.144.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.230.48.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/69072.pdf	Block	1
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.120.17.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.3.13	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
2.54.162.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.28.20	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
149.88.153.140	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 149.88.153.140	Block	1
41.238.106.134	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
185.56.145.15	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
31.210.186.143	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1

12-27-2015-19:04:02 to 12-27-2015-20:04:02