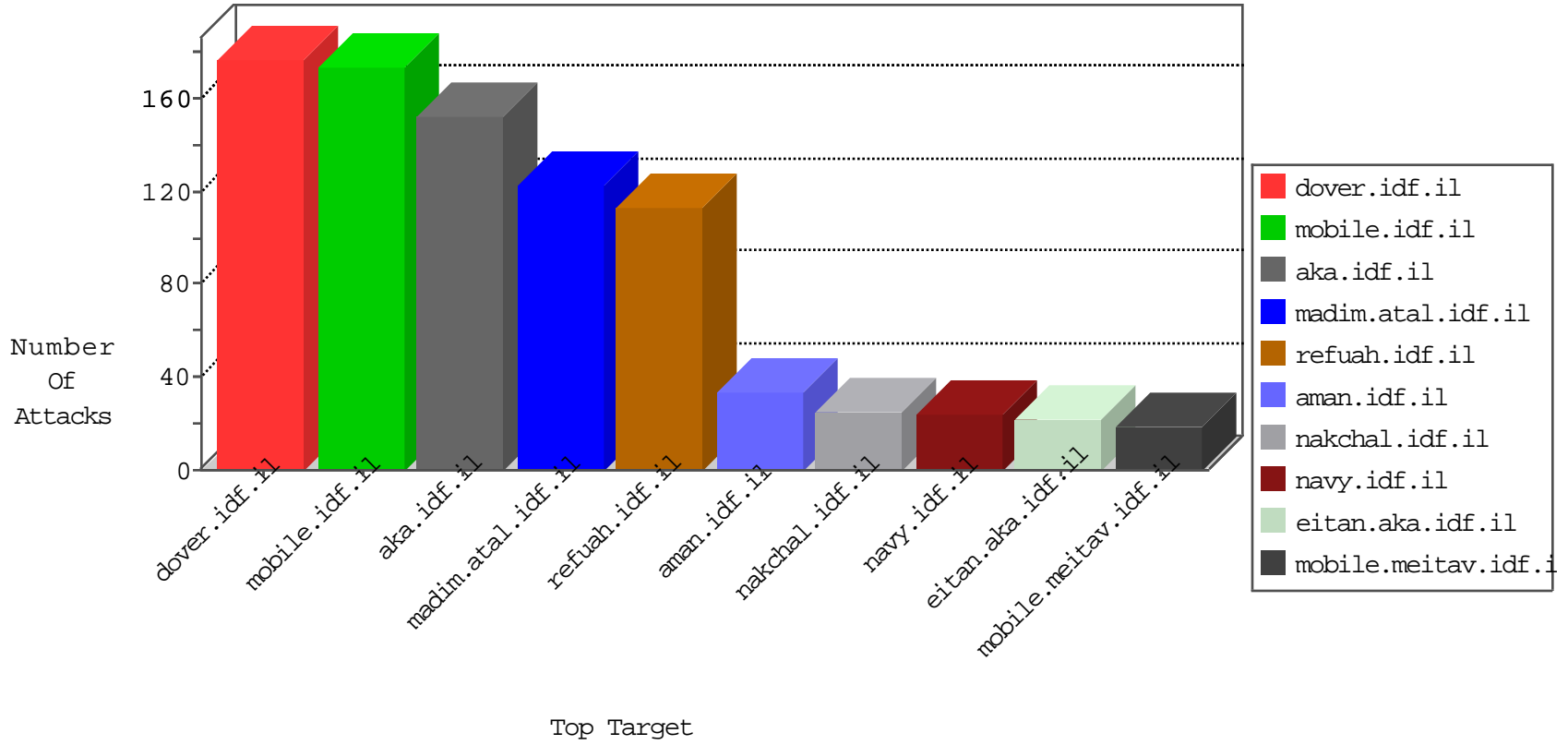


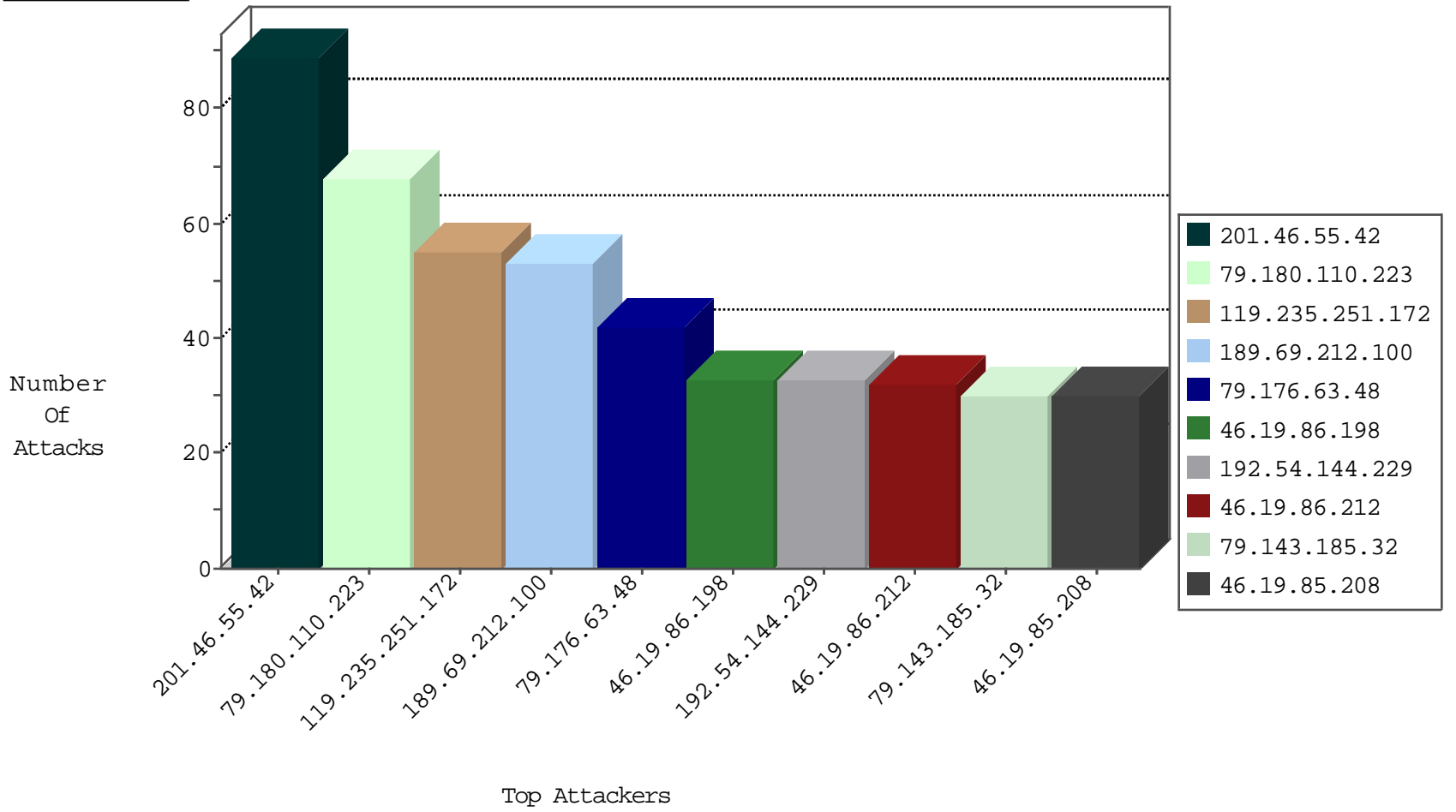
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.236	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
79.183.30.220	Israel	147.237.76.42	refuah.idf.il	Black List	drop	6
109.253.216.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
115.230.125.146	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
154.16.199.217	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
91.230.107.174	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1

08-31-2016-19:04:03 to 08-31-2016-20:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.121.185	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	13
190.196.178.78	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
180.97.106.37	147.237.76.39	China	mobile.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.232.98.38	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
95.163.144.203	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.103.150.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
222.254.34.165	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 1024	1
212.116.72.226	147.237.72.166	Sweden	aka.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.178.78	147.237.0.34	Chile	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
104.232.98.38	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.38	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
95.163.144.203	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.189.163.119	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.254.34.165	147.237.76.44	Vietnam	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.110.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
79.176.63.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
192.54.144.229	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.86.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
89.139.176.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
177.10.170.132	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
2.53.158.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
185.32.179.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
109.253.230.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
84.94.203.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.13.242.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.118.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
65.188.54.230	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.10.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.242.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.216.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
189.69.212.100	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
189.69.212.100	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
24.113.56.62	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
95.163.144.203	Russian Federation	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
119.235.251.172	Indonesia	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
189.69.212.100	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.32.179.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
189.69.212.100	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
73.98.27.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.176.24.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
119.235.251.172	Indonesia	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
177.10.170.132	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
119.235.251.172	Indonesia	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
119.235.251.172	Indonesia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
189.69.212.100	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
119.235.251.172	Indonesia	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
189.69.212.100	Brazil	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
176.13.0.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
82.134.237.247	Netherlands	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 82.134.237.247	Block	4
176.228.134.122	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	4
89.139.176.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.127.81.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.109.146.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.181.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	3
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteychayal/	Block	3
176.13.242.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.180	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.110.223	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
213.57.157.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.57.157.177	Block	2
77.138.22.9	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
109.253.230.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.138.69.110	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	2
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.5.21	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
59.152.202.68	Hong Kong	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
79.180.48.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	1
2.53.140.11	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.102.195.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
80.246.136.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
79.176.63.48	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
94.102.49.190	Netherlands	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/robots.txt	Block	1
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method rr55 in URL	Block	1
82.134.237.247	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
2.55.28.139	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.245.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
85.65.26.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.85.14	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
82.80.60.53	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
185.110.110.37	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.178.125.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.76.102	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
84.108.38.197	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.12.63.226	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.12.63.226	Block	1
213.57.157.177	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
87.69.135.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.183.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
192.54.144.229	France	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1
79.179.96.1	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
69.65.95.155	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar/login/	Block	1
84.109.116.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1