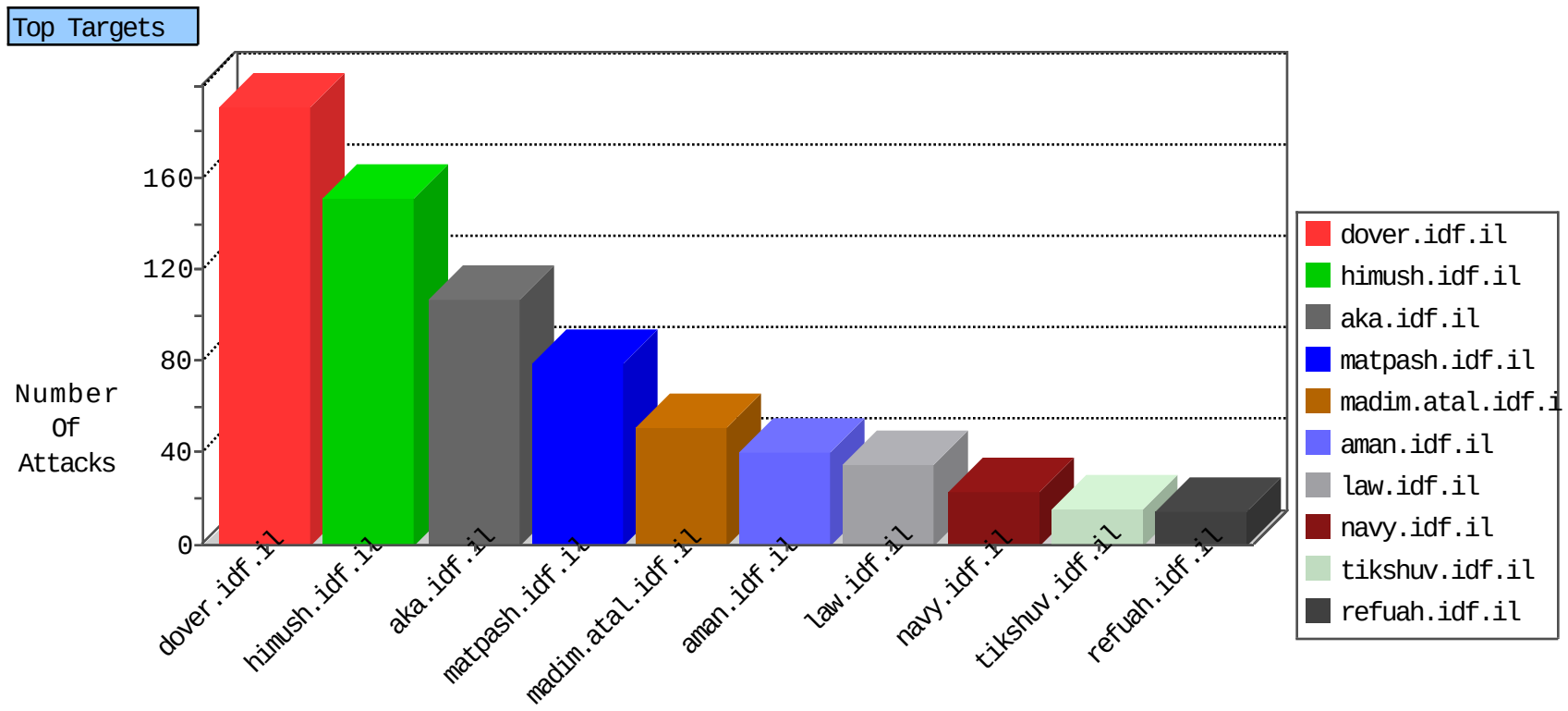
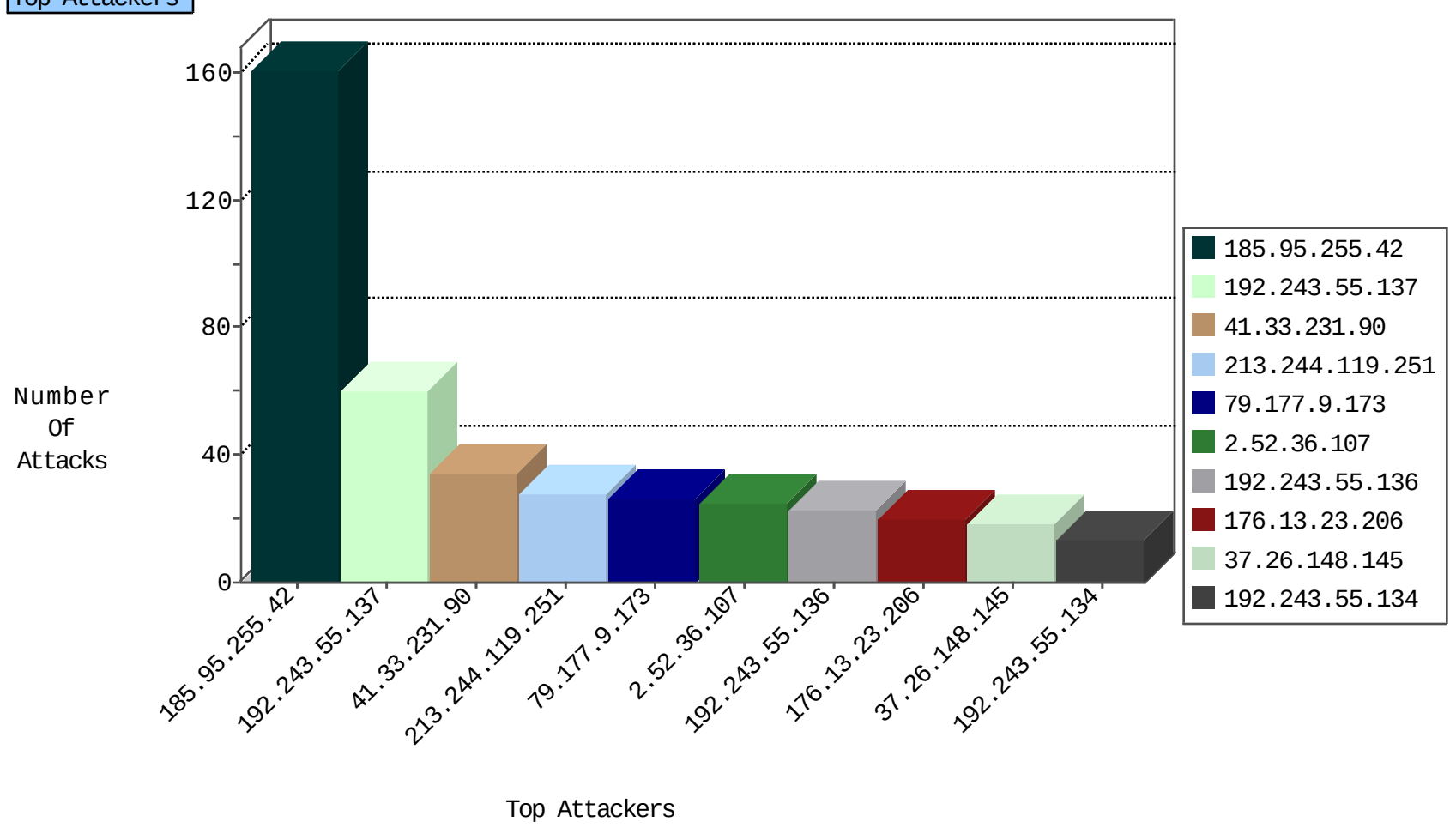
02-18-2016-22:04:03 to 02-18-2016-23:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-18-2016-22:04:03 to 02-18-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.55.235.79	Egypt	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	2
185.130.5.201		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
1.176.134.240	Korea, Republic of	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
1.176.134.240	Korea, Republic of	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
120.26.204.181	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
1.176.134.240	Korea, Republic of	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

02-18-2016-22:04:03 to 02-18-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.120.134.202	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
91.230.195.63	Bulgaria	147.237.77.74	law.idf.il	C1000003: HTTP: phpMyAdmin access	Block	3
187.45.195.15	Brazil	147.237.76.31	nakchal.idf.il	C1000003: HTTP: phpMyAdmin access	Block	3
187.45.240.34	Brazil	147.237.77.234	halag.idf.il	C1000003: HTTP: phpMyAdmin access	Block	3
89.218.26.108	Kazakstan	147.237.0.17	m.my-kosher-kravi.idf.il	C1000003: HTTP: phpMyAdmin access	Block	3
187.45.193.174	Brazil	147.237.77.233	atal.idf.il	C1000003: HTTP: phpMyAdmin access	Block	3
37.59.49.14	France	147.237.77.170	maarachot.idf.il	C1000003: HTTP: phpMyAdmin access	Block	3
109.253.137.245	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.132	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
101.201.147.32	China	147.237.76.147	chinuch.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
79.96.116.215	Poland	147.237.77.74	law.idf.il	C1000003: HTTP: phpMyAdmin access	Block	1

02-18-2016-22:04:03 to 02-18-2016-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.95.255.42	147.237.76.30		himush.idf.il	ET SCAN NMAP -sA (2)	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
85.65.49.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
69.160.35.132	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.36.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.63.156	147.237.76.86	Singapore	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.155.43.41	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.214.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.192.6.154	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.38.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.155.43.41	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-18-2016-22:04:03 to 02-18-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.95.255.42		147.237.76.30	himush.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	67
185.95.255.42		147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
79.177.9.173	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	26
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.36.107	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
185.95.255.42		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
213.244.119.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.22.130.69	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.244.119.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.46.39.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.244.119.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.95.255.42		147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.244.118.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.66.60	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
190.240.24.239	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.244.118.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
213.57.225.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.244.119.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	4
46.117.162.127	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
87.68.32.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
190.240.24.239	Colombia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
2.54.5.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.175.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.244.119.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
31.210.186.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.55.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.106.153	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
41.13.220.175	South Africa	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.36.107	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.41.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.185.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.244.119.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
31.210.187.143	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.222.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-18-2016-22:04:03 to 02-18-2016-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.23.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
2.52.161.178	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.52.161.178	Block	4
109.67.38.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.161.178	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
79.177.109.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
79.178.108.209	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
109.253.212.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.108.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	2
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.176.136.244	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/994-8516-he/himush.aspx#.vsnan78l1bo.facebook	Block	1
212.76.117.131	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dover.aspx&sa=u&ved=0ahukewizjmzhkollahufkw8khqprbzuqfggimaa&sig2=0yjqnon_rs_ddpzxsd5avw&usg=afqjcnhq8auz68olwj3ykex3qddz3y9pnw	Block	1
176.13.23.206	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.23.206	Block	1
79.182.174.30	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.182.106.190	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
197.38.197.170	Egypt	147.237.76.147	chinuch.aka.idf.i	Distributed PHP Attempt	Block	1
109.224.91.229	Czech Republic	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
31.147.125.165	Croatia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
212.179.3.44	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/xmlrpc.php	Block	1
185.24.206.53	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
79.182.174.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
197.38.197.170	Egypt	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
109.224.91.229	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
31.147.125.165	Croatia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
213.57.225.34	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcbwvzahvsyxzcdgfryw5vdf9oyxrhyxz1cmfcmi5wzgy=&infocenteritem=true	Block	1
95.86.66.182	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.79.106	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
104.128.144.131	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/redirect.php	Block	1
77.127.196.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.117.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx	None	1
79.181.113.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$hiddenUpdatePassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
40.77.167.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1

02-18-2016-22:04:03 to 02-18-2016-23:04:03