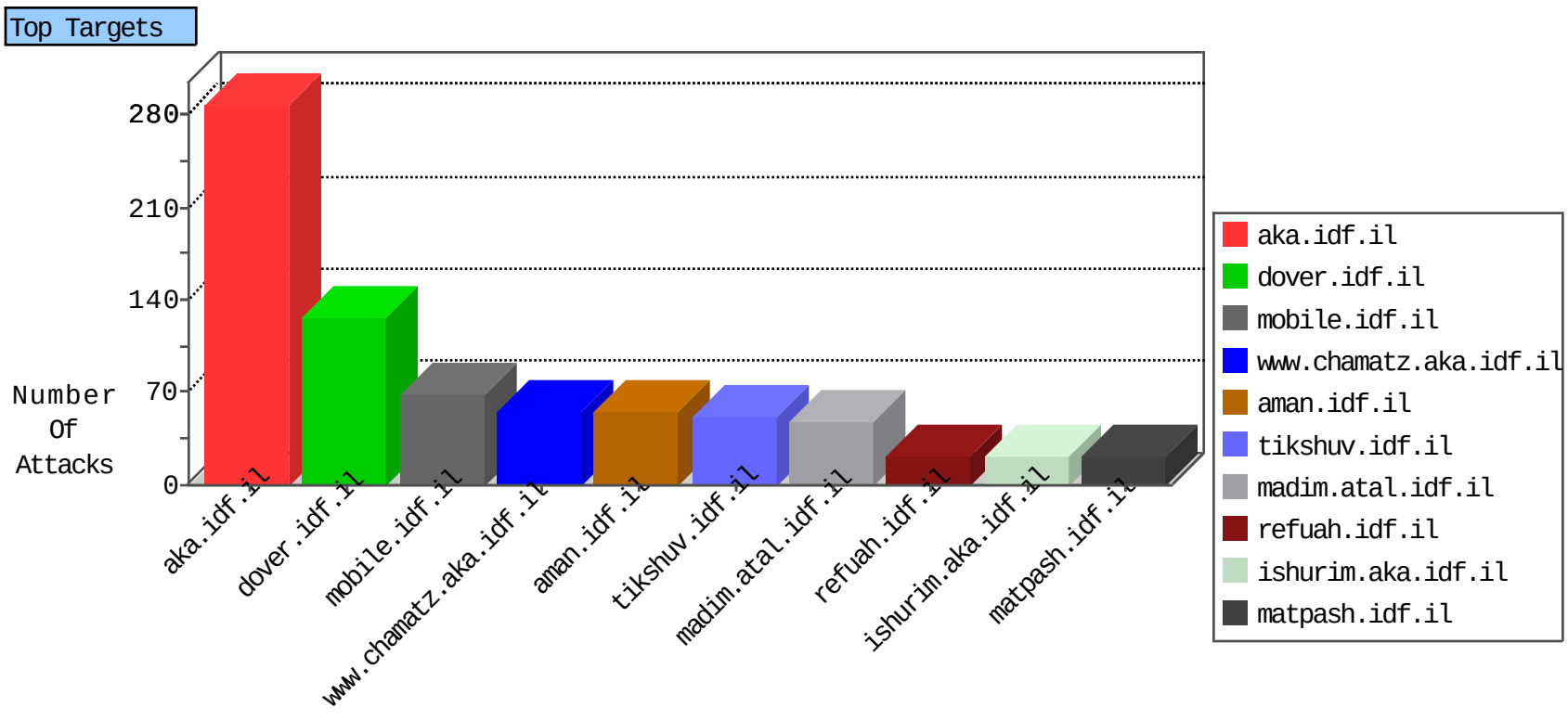
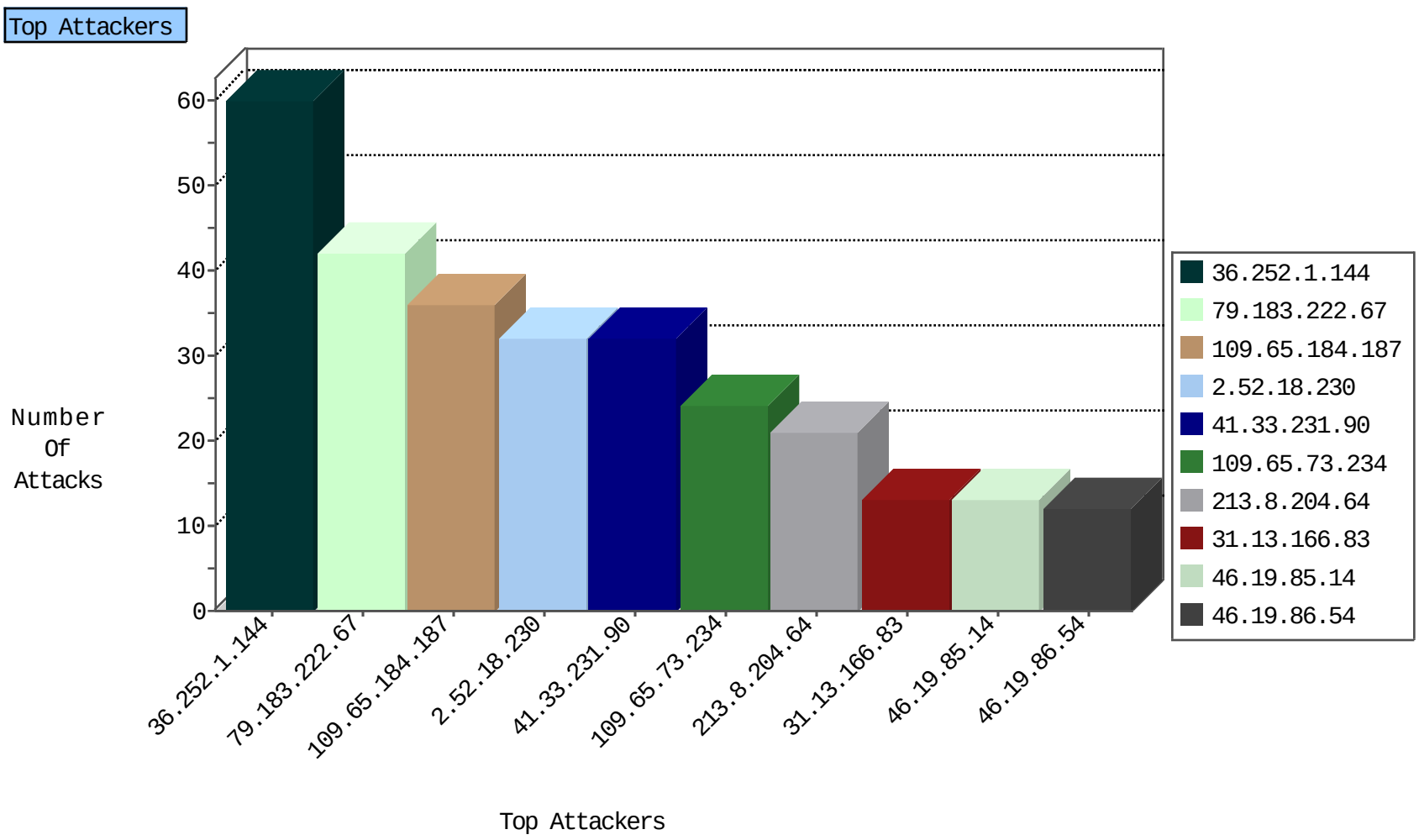
02-11-2016-20:04:01 to 02-11-2016-21:04:01

IDF Under Attack
Daily Report





02-11-2016-20:04:01 to 02-11-2016-21:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.30.2	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.176.183.116	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
142.54.169.165	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
66.249.93.184	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
188.138.17.205	France	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
38.229.1.13	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.62	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
123.186.140.124	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
66.102.9.21	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
185.94.111.1		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
78.189.139.209	Turkey	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.213	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
66.249.93.182	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
185.130.5.224		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-20:04:01 to 02-11-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.13.78	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
31.168.13.78	Israel	147.237.76.86	navy.idf.il	C008: HTTP: Xenu UserAgent	Block	1
31.168.13.78	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-11-2016-20:04:01 to 02-11-2016-21:04:01

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
66.249.93.121	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
123.157.28.185	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.157.28.185	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.157.28.185	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.79.104	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
31.44.128.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.161	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
149.78.240.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
123.157.28.185	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.157.28.185	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.80.198.164	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 4096	1
79.183.225.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.45.137.67	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.242.220.154	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.182.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.36	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1

02-11-2016-20:04:01 to 02-11-2016-21:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.222.67	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
109.65.184.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
36.252.1.144	Nepal	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	29
36.252.1.144	Nepal	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
213.8.204.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
31.13.166.83	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
185.120.126.178		147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
109.65.73.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
5.29.205.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.46.41.126	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
36.252.1.144	Nepal	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.182.226.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.243.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.43.252	Israel	147.237.72.167	ishurim.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
5.22.131.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.7.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.199.38	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
36.252.1.144	Nepal	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.66.37.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.22	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.183.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
149.78.18.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
80.246.136.164	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.78.18.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
24.87.154.112	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.39.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.54	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.41.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
87.69.33.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.46.41.233	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.73.234	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.14	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.179.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.30		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.147.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-11-2016-20:04:01 to 02-11-2016-21:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
149.78.252.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.161.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
83.130.113.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.18.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
79.177.207.89	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
109.253.215.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.23.46	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.23.46	Block	5
213.8.204.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
213.57.253.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	4
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.40.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.23.46	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
80.179.90.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/gryus	Block	2
213.8.204.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.69.33.189	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.65.73.234	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.110.7.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
208.184.77.186	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gyrus	Block	1
149.78.145.167	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.147.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
89.138.243.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.175.224	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
62.0.103.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.176.215.11	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.67.176.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
84.110.7.217	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
212.179.3.44	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1523-en/dover.aspx+idf blog	Block	1
37.142.64.36	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
109.65.26.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.90.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/gyrus	Block	1
66.249.65.22	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
203.176.215.11	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
5.29.205.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.194.83	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
84.110.7.217	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
212.179.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
176.13.15.84	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.142.64.36	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
109.65.73.234	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.65.73.234 (Open Mode)	None	1
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	1
84.108.38.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
31.13.109.116	Ireland	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8938-he/navy.aspx&h=uaqgune4i	Block	1
85.250.35.13	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.177.206.49	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
40.77.167.80	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.65.73.234	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.110.7.217	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1