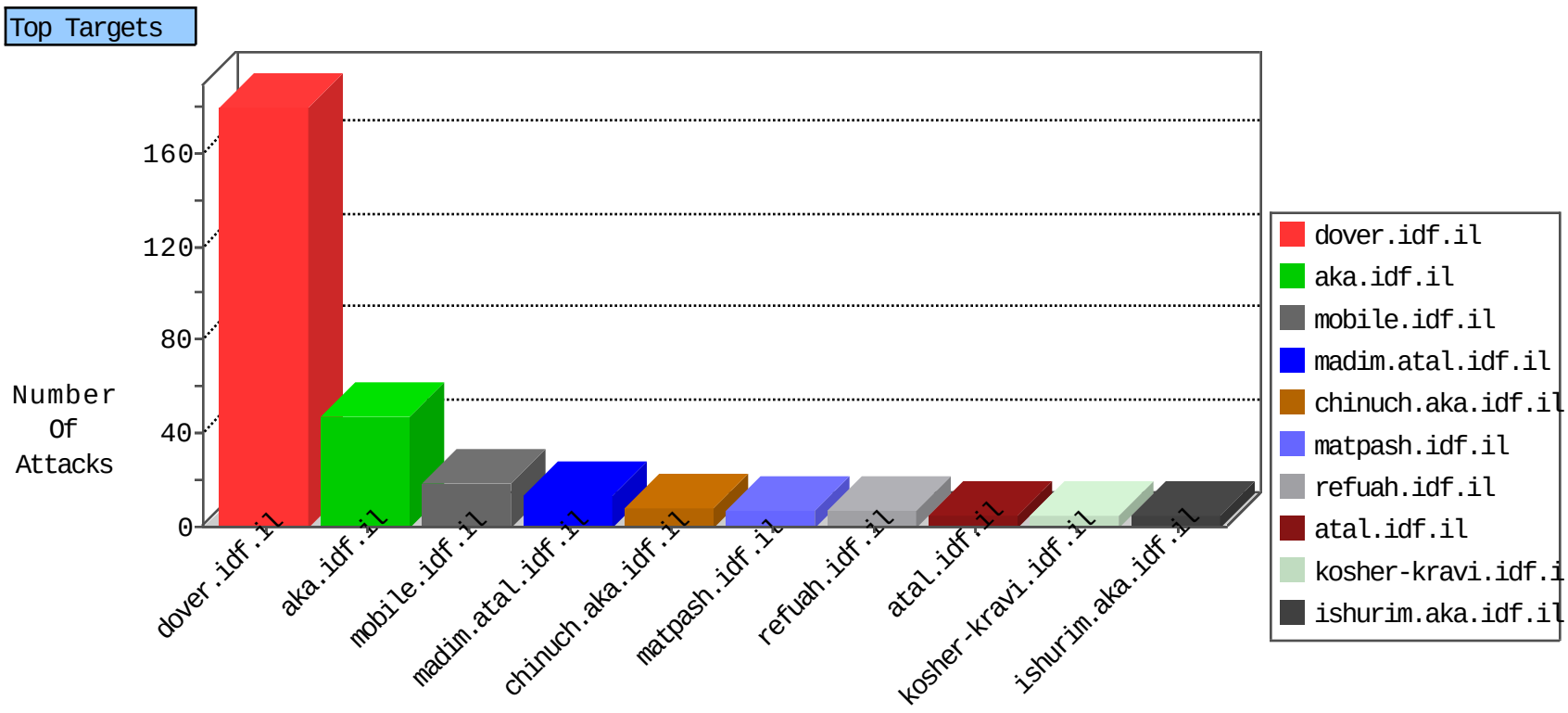
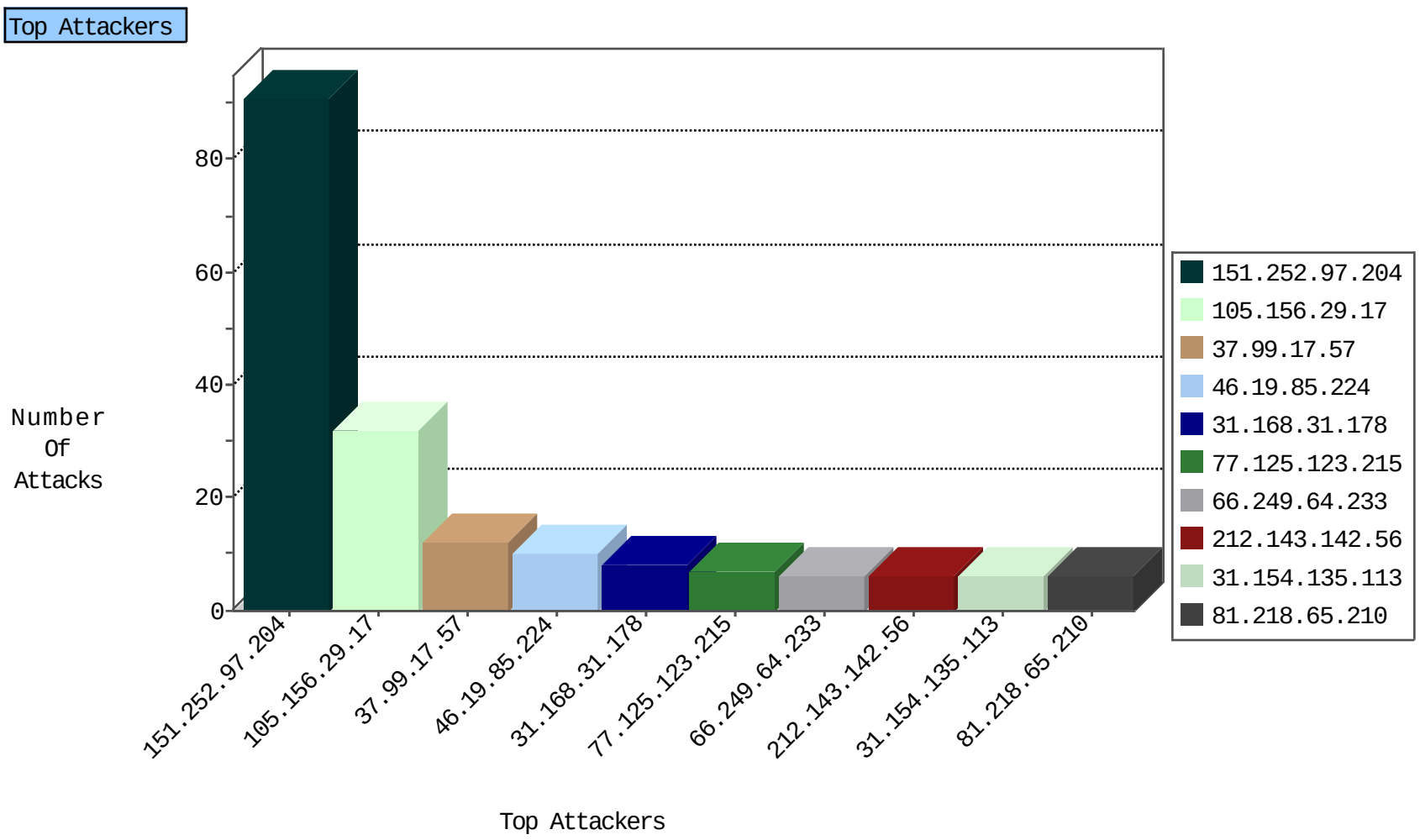
03-06-2016-01:04:57 to 03-06-2016-02:04:57

IDF Under Attack
Daily Report





03-06-2016-01:04:57 to 03-06-2016-02:04:57

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	2
42.112.10.66	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.68	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
61.134.27.52	China	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.70	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.65	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.85	Vietnam	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1

03-06-2016-01:04:57 to 03-06-2016-02:04:57

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.56		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-06-2016-01:04:57 to 03-06-2016-02:04:57

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
209.126.116.147	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
175.43.147.102	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
105.156.29.17	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	1
87.106.255.5	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.106.255.5	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.57.11.7	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
87.106.255.5	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.57.11.7	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.72.156	China	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.34.70.143	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.44.133.108	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
87.106.255.5	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.57.11.7	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
87.106.255.5	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.57.11.7	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.57.11.7	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1

03-06-2016-01:04:57 to 03-06-2016-02:04:57

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.1.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.17.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.46		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
106.38.241.151	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
31.154.135.113	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
83.130.101.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.176.180.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.36.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.77.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
109.65.77.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
70.192.206.168	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.77.167.52	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
31.154.135.113	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
62.128.48.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
62.128.48.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.22.211.69	China	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.38.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.242	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
220.181.108.182	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.111	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
82.114.168.157	Yemen	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.32.179.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.252	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.71.28.43	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
220.181.108.185	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.102.195.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.125.71.111	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
82.114.168.157	Yemen	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

03-06-2016-01:04:57 to 03-06-2016-02:04:57

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.224	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.224	Block	9
77.125.123.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	5
37.99.17.57	Kazakstan	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
37.99.17.57	Kazakstan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.99.17.57	Block	4
83.130.101.9	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
95.86.68.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.68.5	Block	3
66.90.183.203	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.70.2.90	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
31.168.31.178	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
197.35.225.175	Egypt	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
62.219.139.32	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
95.86.68.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17470-he/dover.aspx&sa=u&ved=0ahukewi0-pvx26rlahvrazokhywsd7yqfggamag&usg=afqjcngdvyvnp6we_v_fdfbo5l_kv7vrfa	Block	1
31.168.31.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
37.99.17.57	Kazakstan	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/stylesheet	Block	1
87.71.124.201	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: ctl00$ctl00$ctl00$cphMain$TochenPlaceHolder$mainMiyunPlaceHolder$ctl02$ctl03$ctl03$txtField in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	Block	1
31.168.31.178	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.66.26	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
213.151.47.114	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
62.219.139.32	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
31.168.31.178	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
80.74.107.118	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1218-he/cogat.aspx-ס'יפור	Block	1
66.249.64.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
87.71.124.201	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 87.71.124.201	Block	1
31.168.31.178	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.73.219	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/memorial/pages/shchivdagesh.aspx	Block	1
62.219.139.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
31.168.31.178	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.156.29.17	Block	1
5.29.32.30	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.19.85.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
173.252.74.115	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/1218-he/cogat.aspx-ס'יפור	Block	1
89.139.168.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.31.178	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.75.202	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.90.183.203	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
105.156.29.17	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/upload.php	Block	1
5.29.32.30	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
87.70.2.90	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
197.35.225.175	Egypt	147.237.76.147	chinuch.aka.idf.i	Distributed PHP Attempt	Block	1
62.219.139.32	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
31.168.31.178	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/	Block	1

03-06-2016-01:04:57 to 03-06-2016-02:04:57