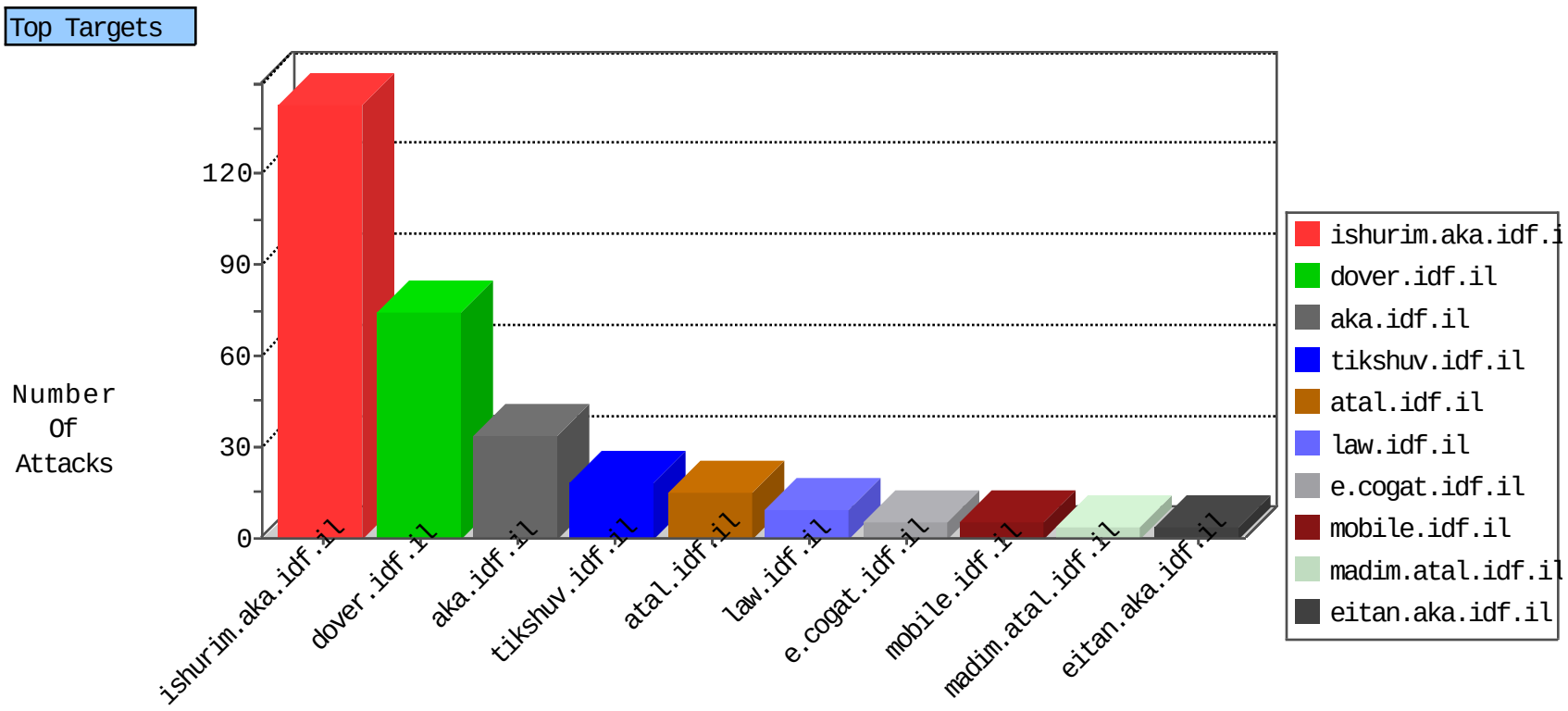
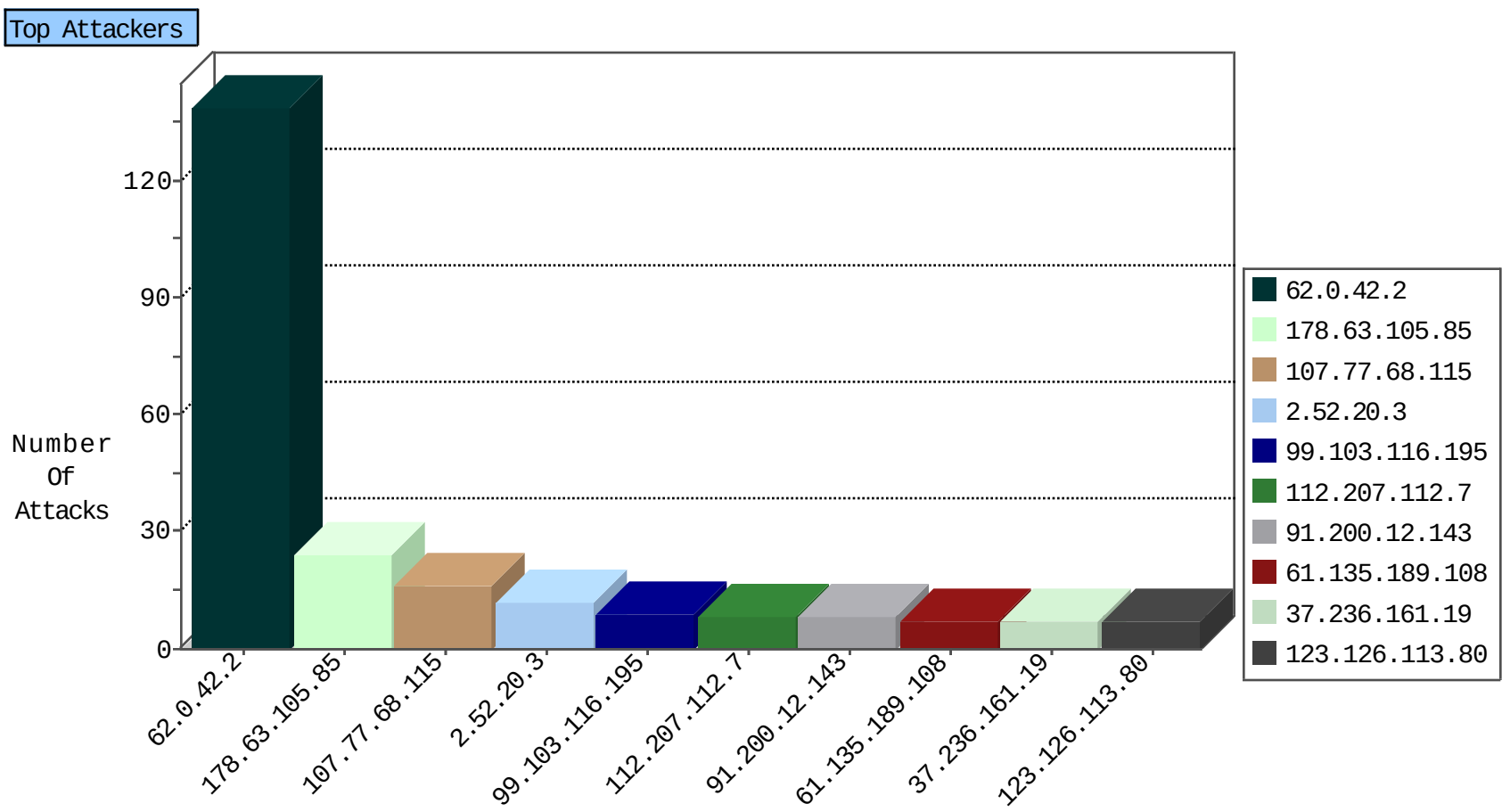
03-07-2016-03:04:06 to 03-07-2016-04:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-03:04:06 to 03-07-2016-04:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
42.112.10.75	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.70	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.93	Vietnam	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.65	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.73	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
185.35.62.109	Switzerland	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
42.112.10.68	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1

03-07-2016-03:04:06 to 03-07-2016-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.20.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
61.135.189.108	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
69.30.234.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
5.29.231.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
173.208.136.170	United States	147.237.76.147	chinuch.aka.idf.il	C1000016: HTTP: administrator in URI	Block	1
173.208.136.170	United States	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
104.168.147.242	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-07-2016-03:04:06 to 03-07-2016-04:04:06

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
104.44.133.108	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
82.117.208.243	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.44.133.108	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.246.29.194	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
196.47.173.21	147.237.76.202	Cote D'Ivoire	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1

03-07-2016-03:04:06 to 03-07-2016-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	67
62.0.42.2	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	67
107.77.68.115	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.205.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	5
99.103.116.195	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	4
79.178.6.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.135.189.108	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
79.182.53.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
62.0.42.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.74.160.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.143	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
199.30.24.130	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.143	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
91.200.12.143	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
99.103.116.195	United States	147.237.77.233	atal.idf.il	Bad TCP sequence		monitor	2
141.212.122.167	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.137	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
103.41.177.26		147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
178.63.105.85	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.170	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.141	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.120	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.126.113.80	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
141.212.122.175	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.168	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.138	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
141.212.122.171	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.160	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.22.135.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
99.103.116.195	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
146.185.239.102	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.168	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.0.42.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.139	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	6
45.56.158.206		147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	3
112.207.112.7	Philippines	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
112.207.112.7	Philippines	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	2
93.173.238.119	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.173.238.119	Block	2
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
141.212.122.129	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /x	Block	1
108.178.118.131	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.236.118.214	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
112.207.112.7	Philippines	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
93.173.238.119	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/console/core/doc_mgr/tel:03-7379500	Block	1
141.212.122.129	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /x	Block	1
75.150.37.122	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.23	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
112.207.112.7	Philippines	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
93.196.111.65	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-15177-he/kkkkkkk=eef15af4kkkkkkk_eef15af4	Block	1
37.142.68.0	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.87.83.83	Ghana	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/headers/tfasim.gif	Block	1
117.78.13.18	China	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
103.21.44.30	Malaysia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
74.131.47.239	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
41.46.3.63	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
112.207.112.7	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
80.87.83.83	Ghana	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.153	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1094-en/hamaz.aspx	Block	1
141.212.122.129	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /x	Block	1
103.21.44.30	Malaysia	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
74.131.47.239	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
41.46.3.63	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
112.207.112.7	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1