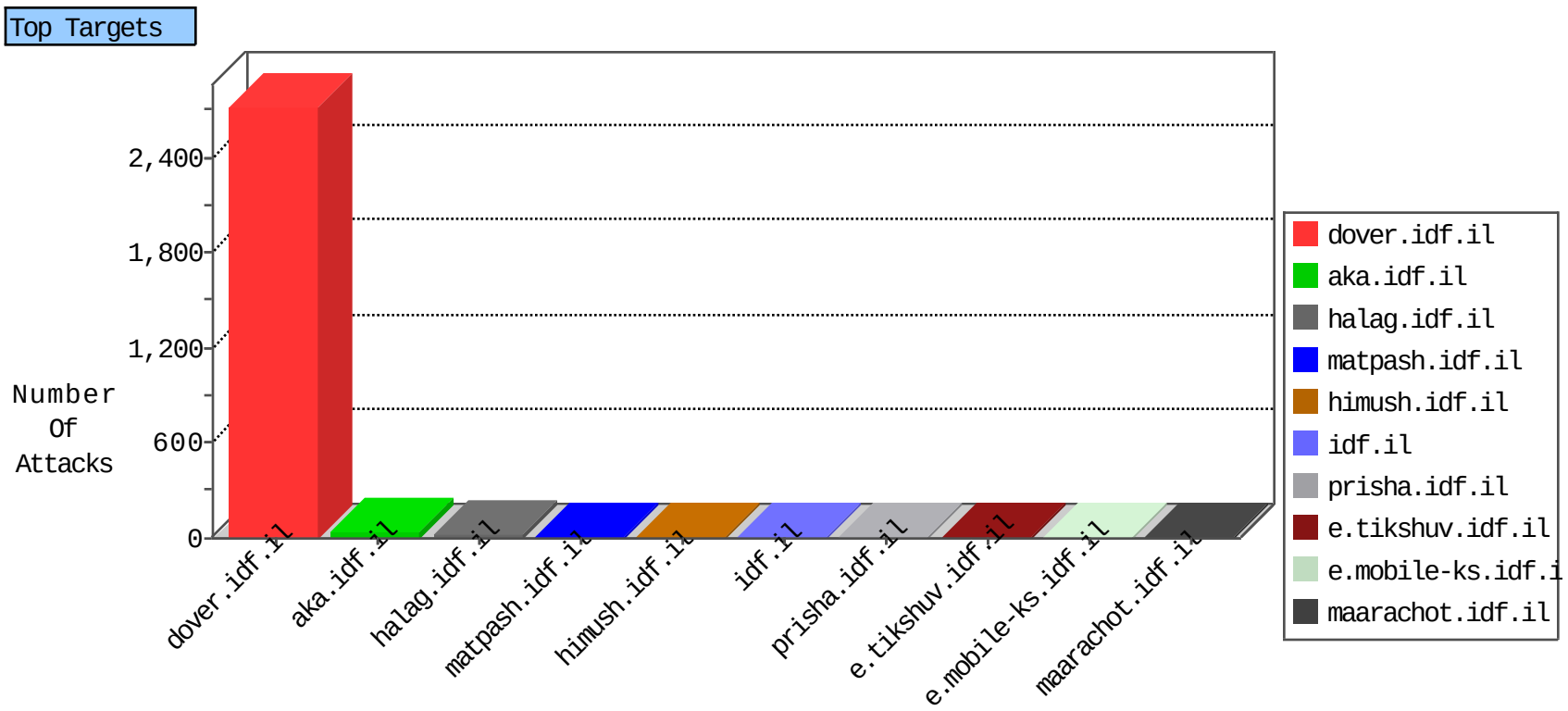
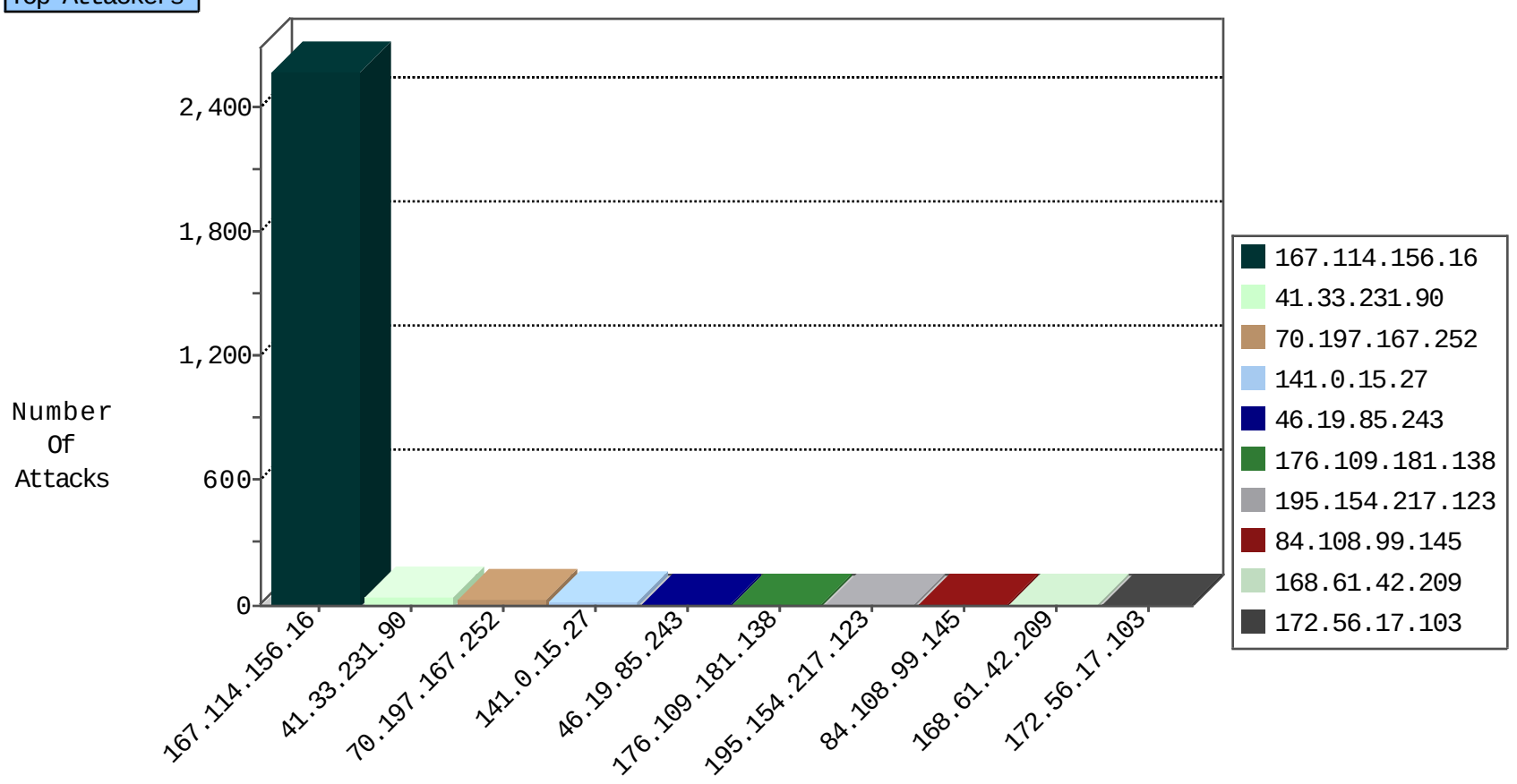
12-02-2015-03:04:03 to 12-02-2015-04:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-02-2015-03:04:03 to 12-02-2015-04:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3598
66.249.66.78	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	72
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.207	Switzerland	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
218.61.132.116	China	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.35.62.50	Switzerland	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.208	Switzerland	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
84.52.18.110	Estonia	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
218.61.132.116	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.35.62.158	Switzerland	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
198.251.81.171	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.188	Switzerland	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

12-02-2015-03:04:03 to 12-02-2015-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.106.94.2		147.237.77.170	maarachot.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
195.154.188.186	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.217.123	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-02-2015-03:04:03 to 12-02-2015-04:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.154.217.123	147.237.77.216	France	dover.idf.il	SERVER-IIS Microsoft Windows IIS 6 multiple executable extension access attempt	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.31	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
195.154.217.123	147.237.77.216	France	dover.idf.il	SERVER-IIS multiple extension code execution attempt	2
195.154.217.123	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Possible Microsoft Internet Information Services (IIS) .asp Filename Extension Parsing File Upload Security Bypas Attempt (asp)	2
14.170.11.133	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
220.133.23.214	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
182.72.242.152	147.237.0.200	India	m4u.idf.il	ET SCAN Potential SSH Scan	1
79.174.70.237	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.130.145.216	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.2	147.237.77.170		maarachot.idf.il	ET WEB_SERVER Muieblackcat scanner	1
88.249.106.23	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.174.70.237	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1

12-02-2015-03:04:03 to 12-02-2015-04:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
141.0.15.27	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
70.197.167.252	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
70.197.167.252	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
70.197.167.252	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
172.56.17.103	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
208.54.86.237	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
70.197.167.252	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
70.197.167.252	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
176.109.181.138	Ukraine	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
2.54.46.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
69.31.50.18	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.175.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.2.101	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.94.49.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.109.181.138	Ukraine	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
176.109.181.138	Ukraine	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.117.14.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.109.181.138	Ukraine	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.108.99.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.94.49.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
64.125.239.101	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.160	United States	147.237.0.33	idf.il	drop		drop	1
84.108.99.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.34	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.138.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.125.239.202	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.182	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.228	United States	147.237.0.33	idf.il	drop		drop	1
64.125.239.136	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.161	United States	147.237.0.33	idf.il	drop		drop	1
84.108.99.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.38	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.61.132.116	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.117.14.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.183	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.254.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.99.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
64.125.239.142	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.172	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.42	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
218.61.132.116	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-02-2015-03:04:03 to 12-02-2015-04:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.61.42.209	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	5
109.67.149.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
64.39.109.20	United States	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 64.39.109.20 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.17	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
208.54.4.199	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.52.111.83	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/3/4213.png	Block	1
176.13.1.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-11039-he/dover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.55	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
52.65.50.136	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=6e94fdb6kkkkkkk_6e94fdb6	Block	1
108.254.121.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1613-15489-he/dover.aspx	Block	1
207.46.13.56	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.249.66.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/x©×§×•×¤x™×ª 3	Block	1
52.65.50.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
197.37.10.159	Egypt	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
207.46.13.103	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
173.254.230.73	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
54.175.3.91	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
197.37.10.159	Egypt	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
124.73.7.208	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1205-he/cogat.aspx/trackback/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
207.46.13.144	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
173.254.230.73	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/blog/wp-login.php	Block	1
68.180.228.170	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

12-02-2015-03:04:03 to 12-02-2015-04:04:03