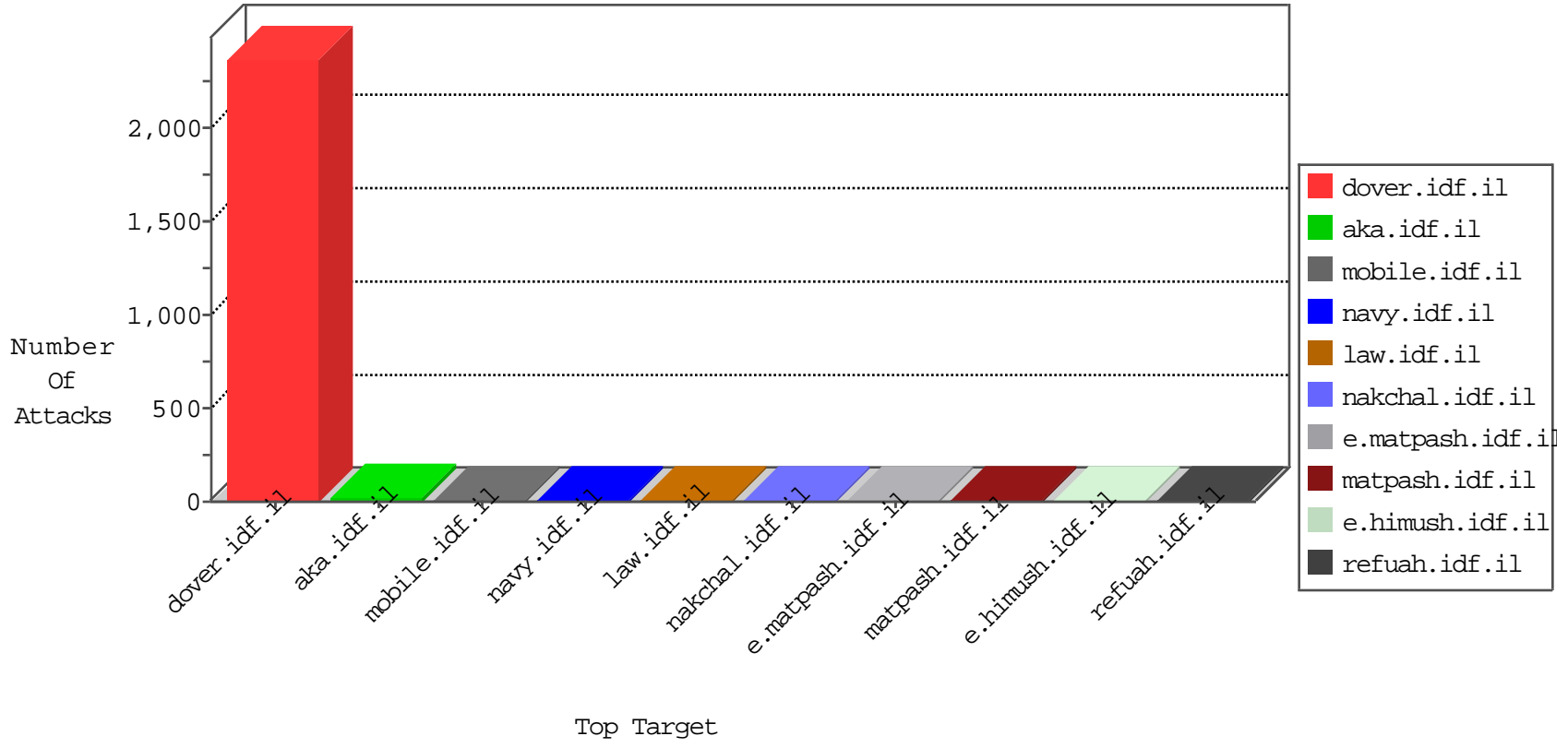


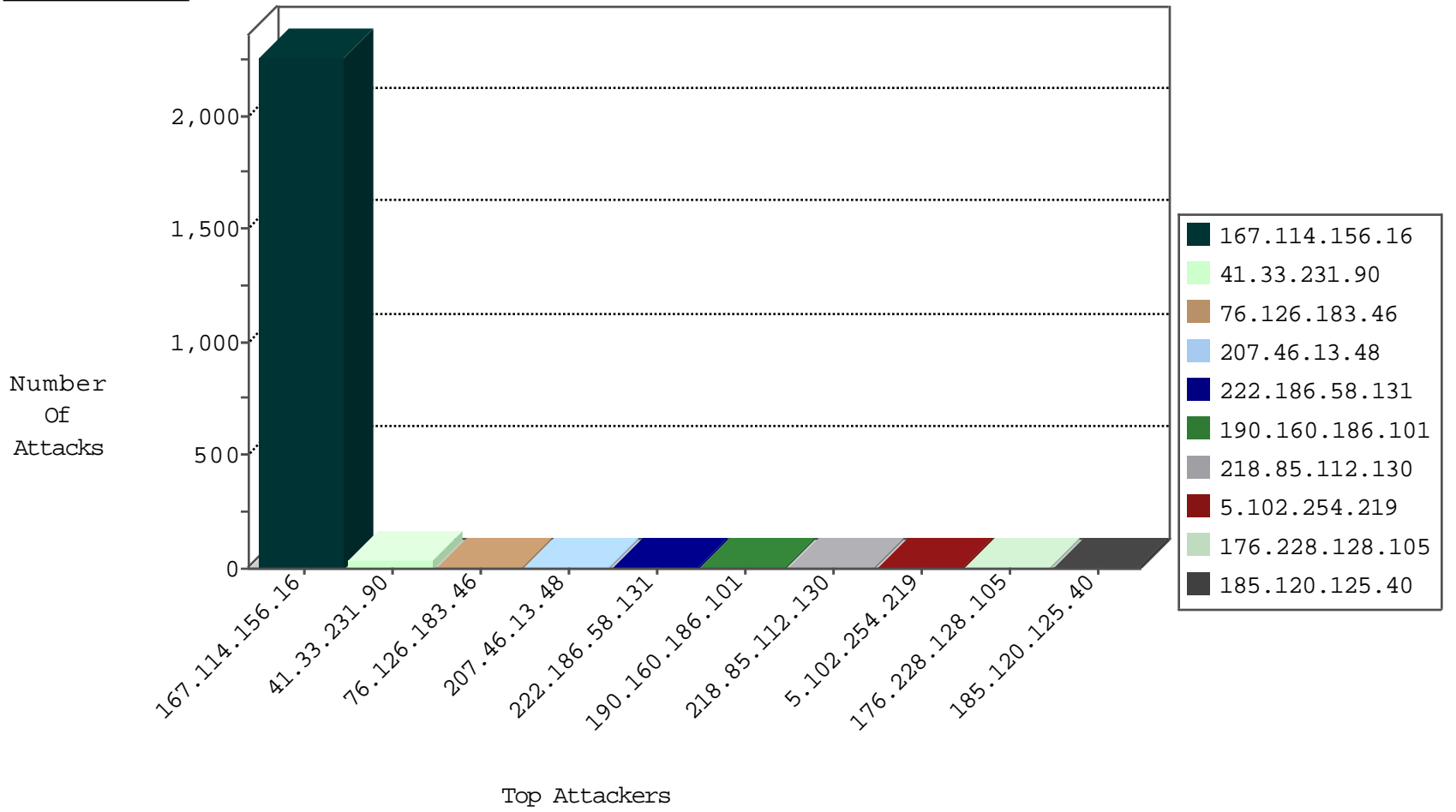
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3523
190.160.186.101	Chile	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
61.147.103.184	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
222.186.58.131	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
94.102.49.122	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.96	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-13-2015-05:04:00 to 12-13-2015-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
218.85.112.130	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
45.79.107.83		147.237.72.167	ishurim.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1

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	3
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
194.187.48.247	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.196	Sweden	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
119.195.228.221	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.200.157.163	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 2048	1
78.193.2.8	147.237.77.243	France	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.147.103.184	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
194.187.48.247	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
175.25.161.169	147.237.76.176	China	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
111.120.99.134	147.237.76.42	China	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.200.157.163	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -f -sS	1

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
76.126.183.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.48	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	10
176.228.128.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.242	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
162.254.122.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.172.147.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.120.125.40		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.65.34.177	Moldova, Republic of	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.230.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
203.133.171.35	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
203.133.168.147	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.133.168.147	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.196	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.96	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.146.200.43	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.206	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
222.186.58.131	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.76.15.13	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.197	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.112	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
24.146.200.43	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
222.186.58.131	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
98.166.87.230	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.36	United States	147.237.0.33	idf.il	drop		drop	1
203.133.168.147	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
182.141.197.116	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.201	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.124	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
92.96.74.124	United Arab Emirates	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
198.20.69.74	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
222.186.58.131	China	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.193	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.79	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.47	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.133.168.147	Korea, Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
182.141.197.116	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.202	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.124	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
40.77.167.77	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
198.20.69.74	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
107.167.112.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	4
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	4
5.102.254.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.15.80	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
185.120.125.40		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.117.2.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
218.85.112.130	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/editor/editor/filemanager/browser/default/connectors/asp/cconnector.asp	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
79.179.99.94	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/news_gaza/pages/kenesrefuee.aspx	Block	1
49.149.167.88	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	1
79.179.99.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17989-he/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
49.149.167.88	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17672.jpg	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
66.220.146.23	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/6255.jpg	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	1
27.186.173.224	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
218.85.112.130	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 218.85.112.130	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	1