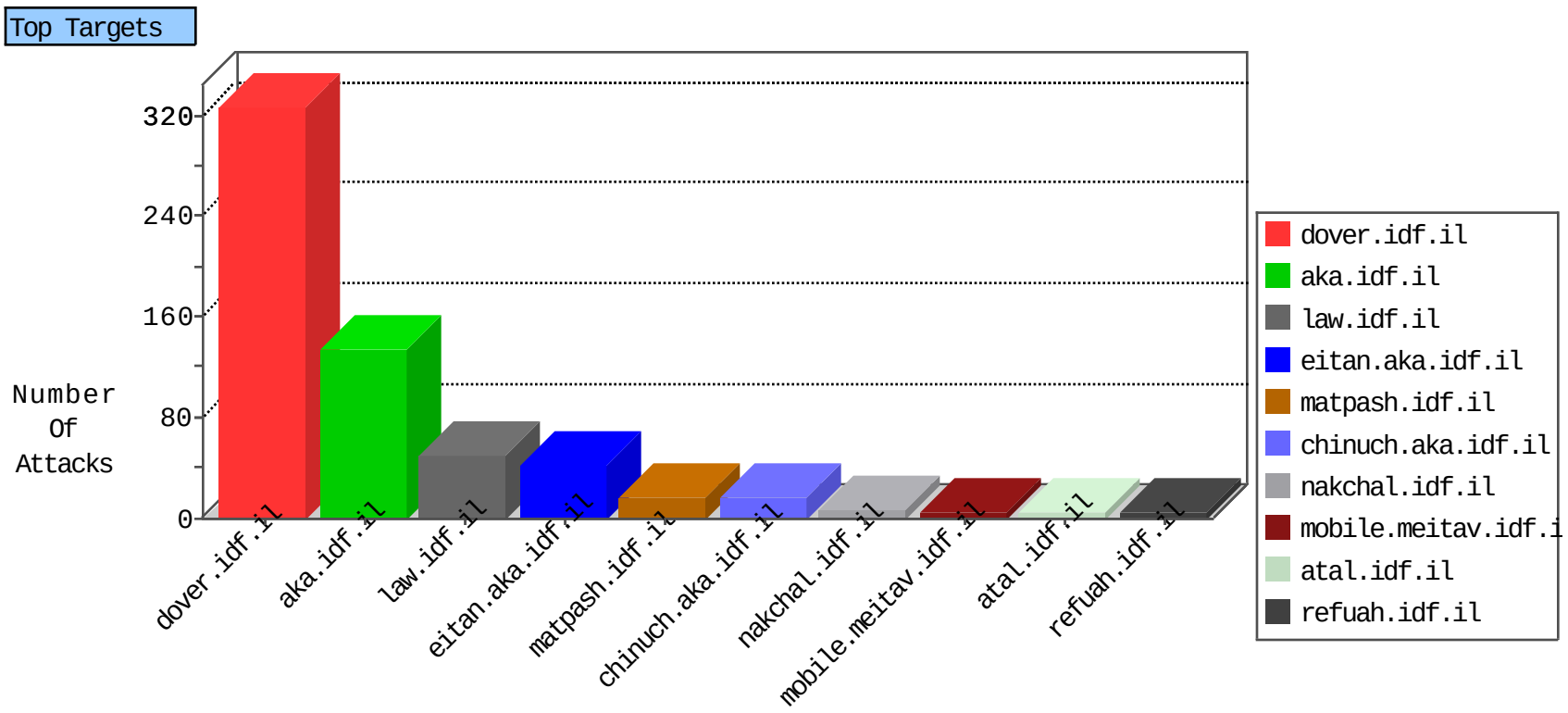
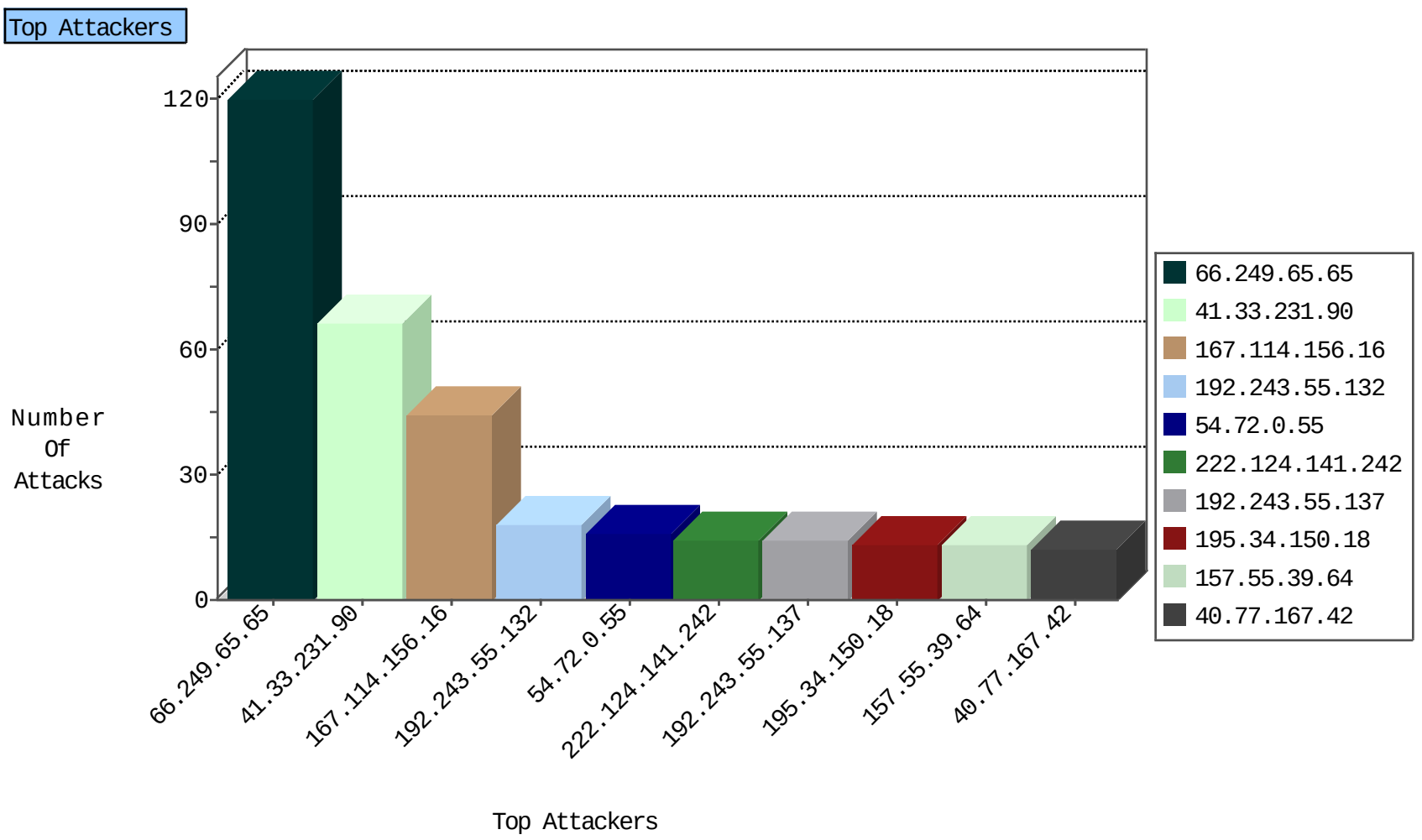
04-22-2016-06:04:07 to 04-22-2016-07:04:07

IDF Under Attack Daily Report





04-22-2016-06:04:07 to 04-22-2016-07:04:07

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	TCP handshake violation, first packet not syn	drop	10036
64.46.23.242	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4417
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
66.240.219.146	United States	147.237.76.196	e.sviva.idf.i	Block_Udp_All_Nets	drop	1

04-22-2016-06:04:07 to 04-22-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
67.228.38.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
210.72.142.101	China	147.237.76.39	mobile.meitav.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
210.72.142.101	China	147.237.0.19	madim.atal.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
210.72.142.101	China	147.237.76.31	nakchal.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-22-2016-06:04:07 to 04-22-2016-07:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
67.228.38.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
1.224.251.8	147.237.76.199	Korea, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
1.224.251.8	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	2
69.175.85.2	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
1.224.251.8	147.237.76.176	Korea, Republic of	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
69.175.85.2	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.224.251.8	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
58.218.211.11	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
1.224.251.8	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
210.72.142.101	147.237.76.39	China	mobile.meitav.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
58.218.211.11	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
1.224.251.8	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
210.72.142.101	147.237.0.19	China	madim.atal.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
46.8.45.97	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.8.45.97	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
104.214.73.227	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.8.45.97	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
69.175.85.2	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
13.82.25.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
69.175.85.2	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
1.224.251.8	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1
69.175.85.2	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
1.224.251.8	147.237.76.147	Korea, Republic of	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.211.11	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
1.224.251.8	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
210.72.142.101	147.237.76.31	China	nakchal.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
58.218.211.11	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
201.200.19.78	147.237.8.28	Costa Rica	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.8.45.97	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.86	147.237.77.121	Lithuania	e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.8.45.97	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.25.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
69.175.85.2	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-22-2016-06:04:07 to 04-22-2016-07:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
222.124.141.242	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
40.77.167.42	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
88.167.248.145	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.64	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.186.41.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
66.249.64.182	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
172.56.42.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
108.206.252.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.98	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.187	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
166.137.252.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
137.28.230.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.246.49.97	France	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
131.253.25.240	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
212.33.115.82	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
172.56.42.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.64	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
110.84.24.164	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.73.132	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.64.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.117.208.243		147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
207.46.13.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-22-2016-06:04:07 to 04-22-2016-07:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6
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	3
104.152.185.185	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.152.185.185	Block	2
42.96.140.102	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	2
82.117.208.243		147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
213.133.110.35	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.249.64.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/course_photos.asp	Block	1
104.152.185.185	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
42.96.140.102	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 42.96.140.102	Block	1
88.73.5.16	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.98	United States	147.237.76.200	eitan.aka.idf.i	Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
68.180.231.61	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
89.139.129.36	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 89.139.129.36	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
207.46.13.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
69.58.178.57	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
42.96.140.102	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
89.139.129.36	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
66.249.65.231	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

04-22-2016-06:04:07 to 04-22-2016-07:04:07