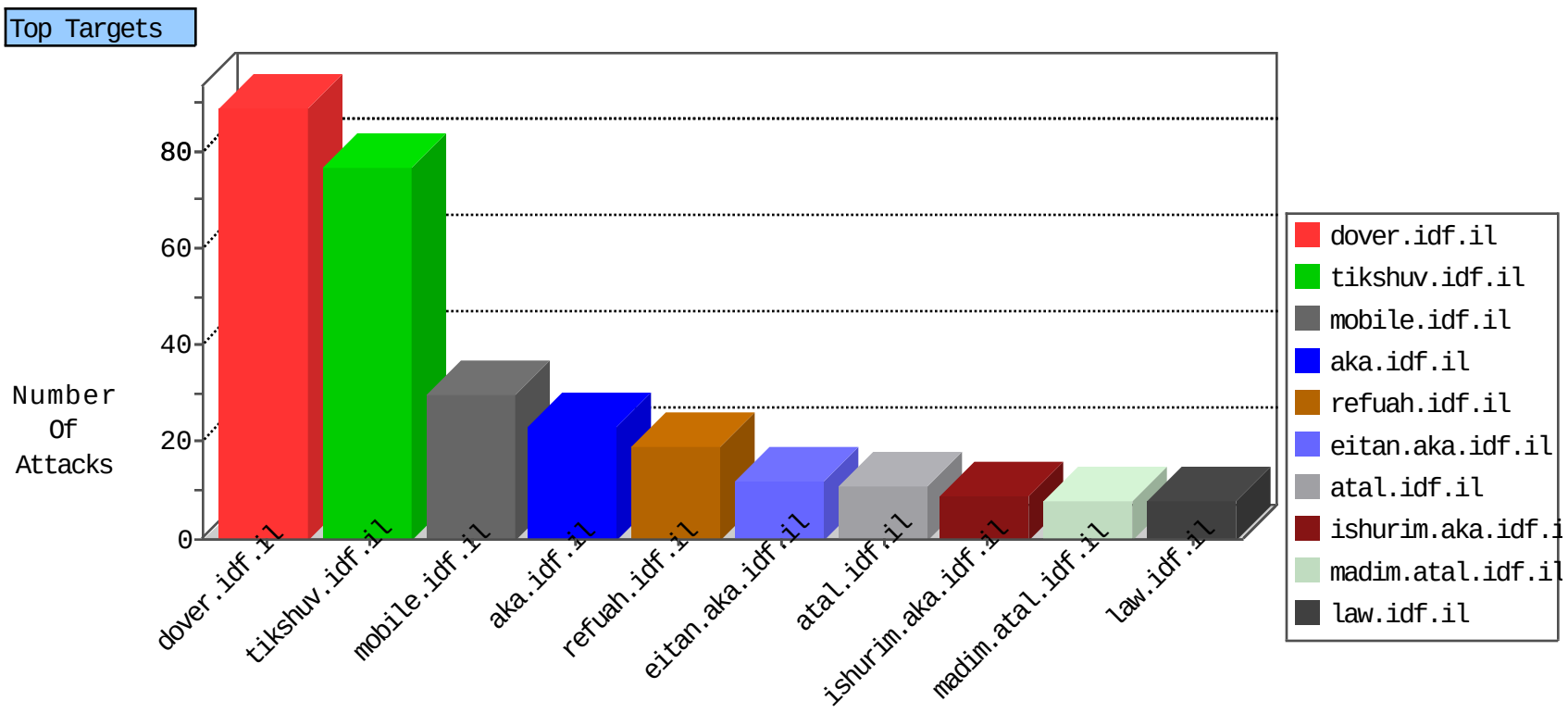
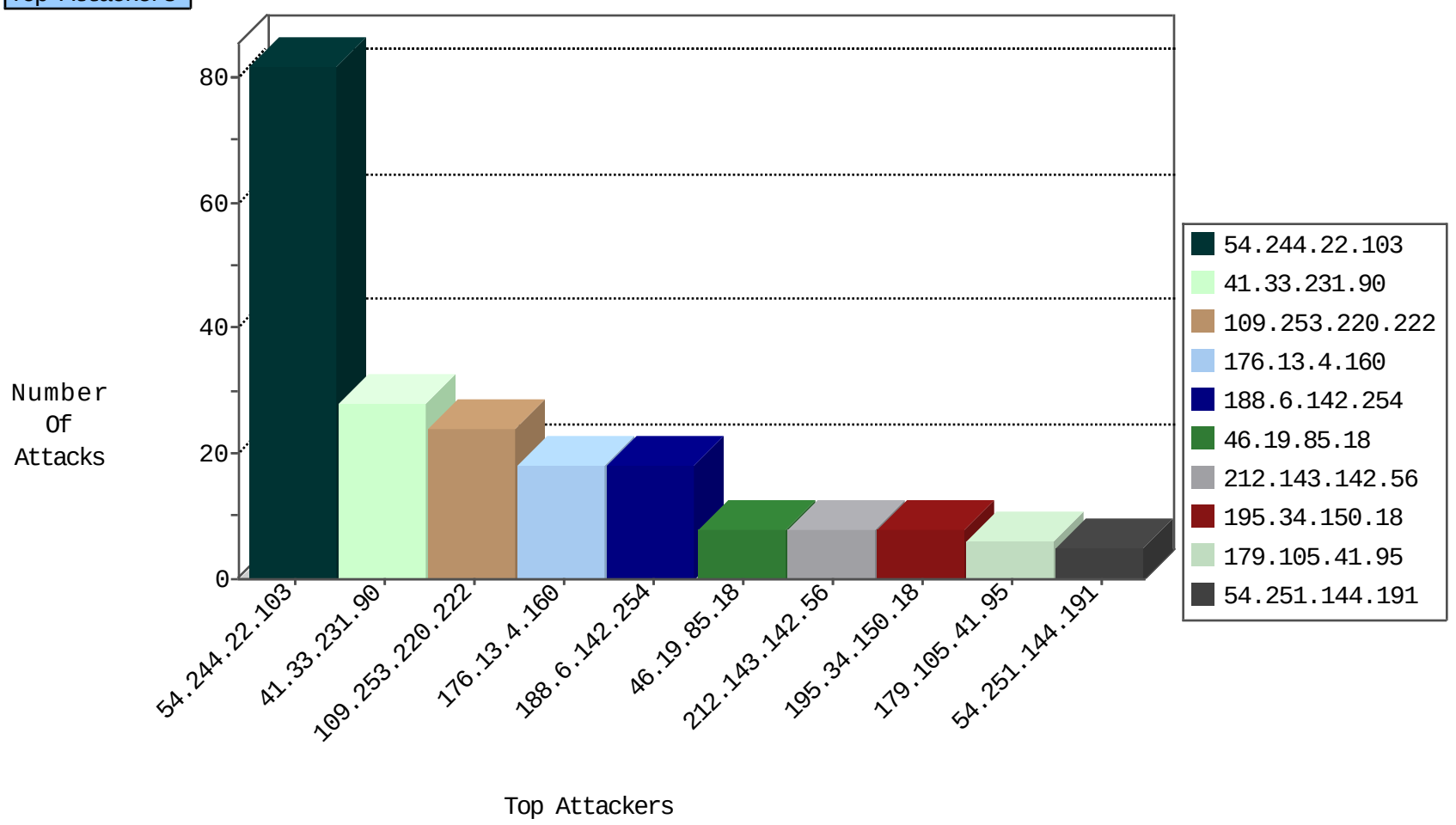
02-05-2016-02:04:07 to 02-05-2016-03:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-05-2016-02:04:07 to 02-05-2016-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.221.28.107	Bosnia and Herzegovina	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
179.105.41.95	Brazil	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
192.223.27.11	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
77.221.28.107	Bosnia and Herzegovina	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
179.105.41.95	Brazil	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
77.221.28.107	Bosnia and Herzegovina	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
179.105.41.95	Brazil	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
179.105.41.95	Brazil	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
77.221.28.107	Bosnia and Herzegovina	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
179.105.41.95	Brazil	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
179.105.41.95	Brazil	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

02-05-2016-02:04:07 to 02-05-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.69.240.221	Hong Kong	147.237.76.147	chinuch.aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
202.69.240.221	Hong Kong	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.60	France	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
202.69.240.221	Hong Kong	147.237.0.15	kosher-kravi.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

02-05-2016-02:04:07 to 02-05-2016-03:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.128.144.131	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -f -sS	1
87.154.134.212	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
71.122.164.179	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.6.142.254	147.237.76.148	Hungary	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
114.35.204.196	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -sS window 2048	1
93.104.213.84	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.76.39	Turkey	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
121.165.121.35	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1

02-05-2016-02:04:07 to 02-05-2016-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	74
109.253.220.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.13.4.160	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
188.6.142.254	Hungary	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
46.19.85.18	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.233	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
40.77.167.20	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.154.246	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.5.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.133.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.159.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.217	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.65.85	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.50.50.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.161	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
147.235.8.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.146	United States	147.237.76.202	e.halag.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
141.212.122.73	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.6.142.254	Hungary	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.128.144.131	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.228.144.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.150	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.119	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
41.234.116.195	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.66	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.6.142.254	Hungary	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
147.235.8.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.146	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.74	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.6.142.254	Hungary	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.253.132.214	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.36	China	147.237.76.39	mobile.meitav.idf.i	drop	SAM rule	drop	1
141.212.122.151	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.217	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.125	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.73.250.221	Taiwan	147.237.72.156	aman.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
42.62.74.70	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.66	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-05-2016-02:04:07 to 02-05-2016-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.41.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.116.164.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.121	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	2
176.13.20.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.84.21	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1511-he/atal.aspx	Block	2
109.67.128.54	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
188.6.142.254	Hungary	147.237.76.42	refuah.idf.il	Illegal HTTP Version the green fields outside. Watch the goats chewing the grass. What is the meaning of life? Life isn't about getting to the end Goats know this. You should know too. Goats are wise. Goats are cute. Listen to them! This is the message. Love goats, love the Internet! ðŸ?? Kecske. HTTP/1.0	Block	1
79.183.198.251	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.183.198.251	Block	1
54.251.144.191	Singapore	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
146.185.234.48	Russian Federation	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/994-he/refuah.aspx	Block	1
40.77.167.51	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
188.6.142.254	Hungary	147.237.76.42	refuah.idf.il	Malformed URL towards	Block	1
79.183.198.251	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/menustrech.png"	Block	1
66.249.65.82	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/links/links.aspx	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
40.77.167.94	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
203.73.250.221	Taiwan	147.237.72.156	aman.idf.il	E-mail collector robots 14	Block	1
83.130.108.242	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.66.132	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter lang in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
203.73.250.221	Taiwan	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
188.6.142.254	Hungary	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
54.251.144.191	Singapore	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1

02-05-2016-02:04:07 to 02-05-2016-03:04:07