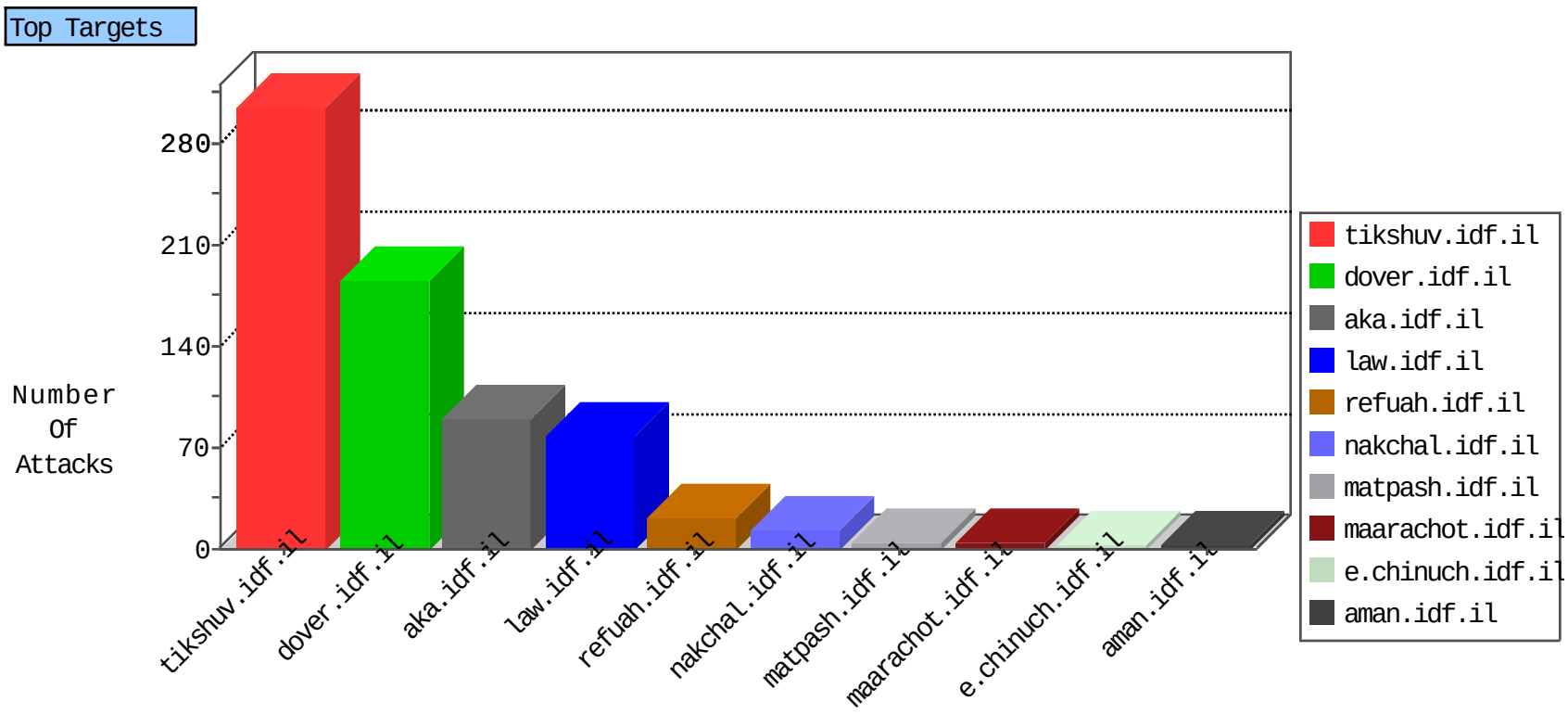
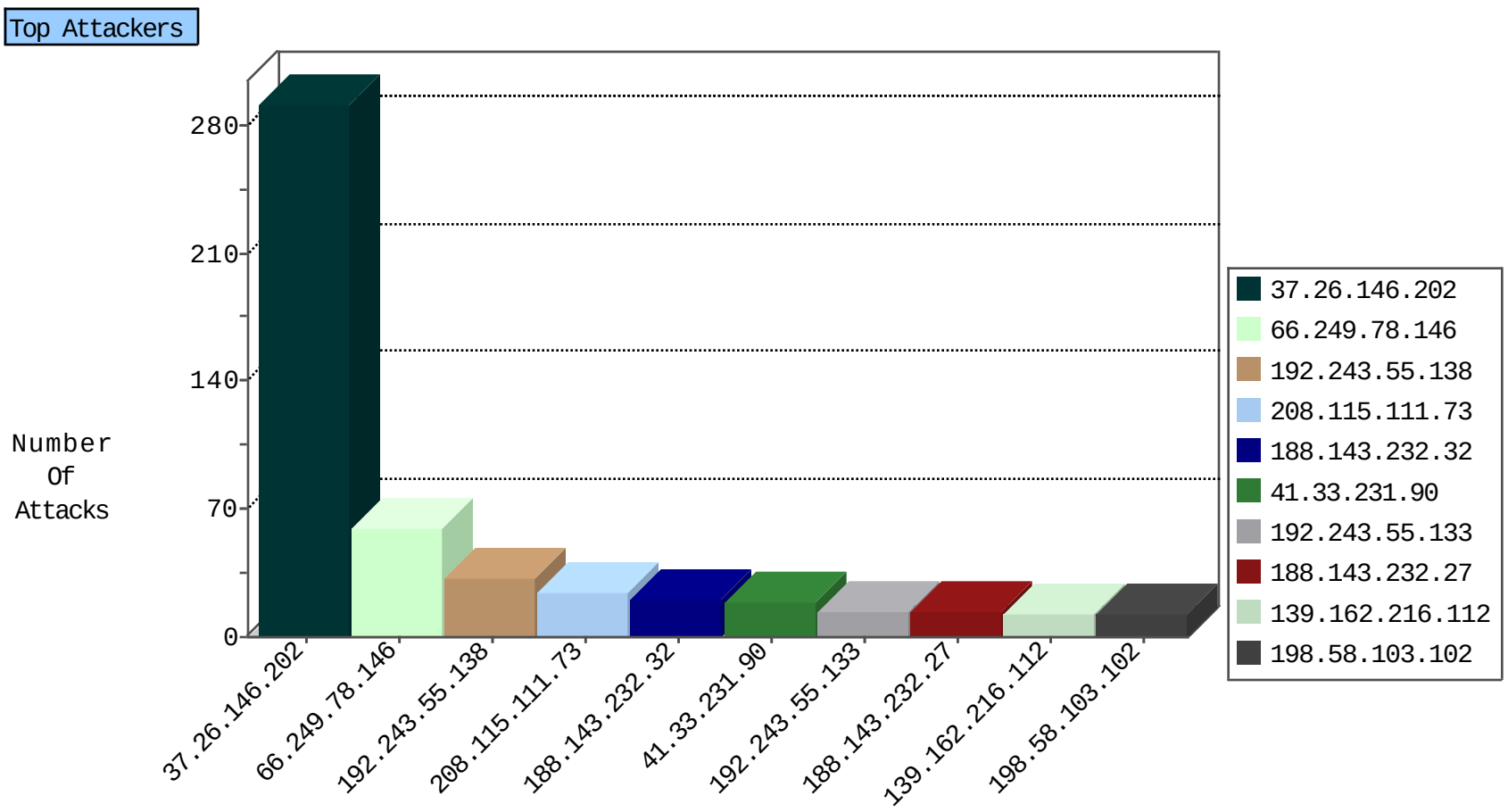
04-24-2016-06:04:09 to 04-24-2016-07:04:09

IDF Under Attack Daily Report





04-24-2016-06:04:09 to 04-24-2016-07:04:09

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	6732
37.26.146.202	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	6367
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
69.30.202.228	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
71.6.146.185	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-24-2016-06:04:09 to 04-24-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.165.24.123	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.249.107.200	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
216.249.102.198	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

04-24-2016-06:04:09 to 04-24-2016-07:04:09

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	9
216.249.107.200	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	9
84.245.33.104	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
174.37.194.144	147.237.76.31	United States	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
13.82.25.17	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
174.37.194.144	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
104.171.122.176	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.176	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.189.248	147.237.8.14	France	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
13.92.245.177	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
13.82.25.17	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.17.13	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1

04-24-2016-06:04:09 to 04-24-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.202	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	287
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.215.252	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
188.143.234.155	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.102.6.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.143.232.32	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.210.226.9	France	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
97.74.24.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
157.55.39.128	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.0	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.72.215.18	United Kingdom	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.90.167.38	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.72.215.18	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.238	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.72.215.18	United Kingdom	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.143.232.32	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/sendtofriend	Block	7
188.143.232.32	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/sendtofriend	Block	5
188.143.232.32	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	4
187.44.148.42	Brazil	147.237.77.74	law.idf.il	PHP Attempt	Block	2
188.143.234.155	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/sendtofriend	Block	2
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
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	2
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
174.37.194.144	United States	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 174.37.194.144 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
82.166.190.11	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
37.26.149.229	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/456-en/patzar.aspx.	Block	1
208.115.111.71	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
174.37.194.144	United States	147.237.76.31	nakchal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.200.54.76	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.102.6.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
187.44.148.42	Brazil	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
157.55.39.213	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/eitan/mesiratmeida/	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
216.218.206.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
107.200.54.76	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/wp-login.php	Block	1
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
187.44.148.42	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
157.55.39.213	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/giyus/giyus/general.aspx	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/kkkkkkk=166321a5kkkkkkk_166321a5	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
187.44.148.42	Brazil	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 187.44.148.42	Block	1
157.55.39.213	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/iturim/iturim.aspx	None	1
5.102.252.140	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/mobile	Block	1
188.143.232.27	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
187.44.148.42	Brazil	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 187.44.148.42	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/general.aspx	Block	1
66.249.64.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding j.e[8l2tEjLR>S>2vSL;*$zzuM(&4WRz in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1

04-24-2016-06:04:09 to 04-24-2016-07:04:09