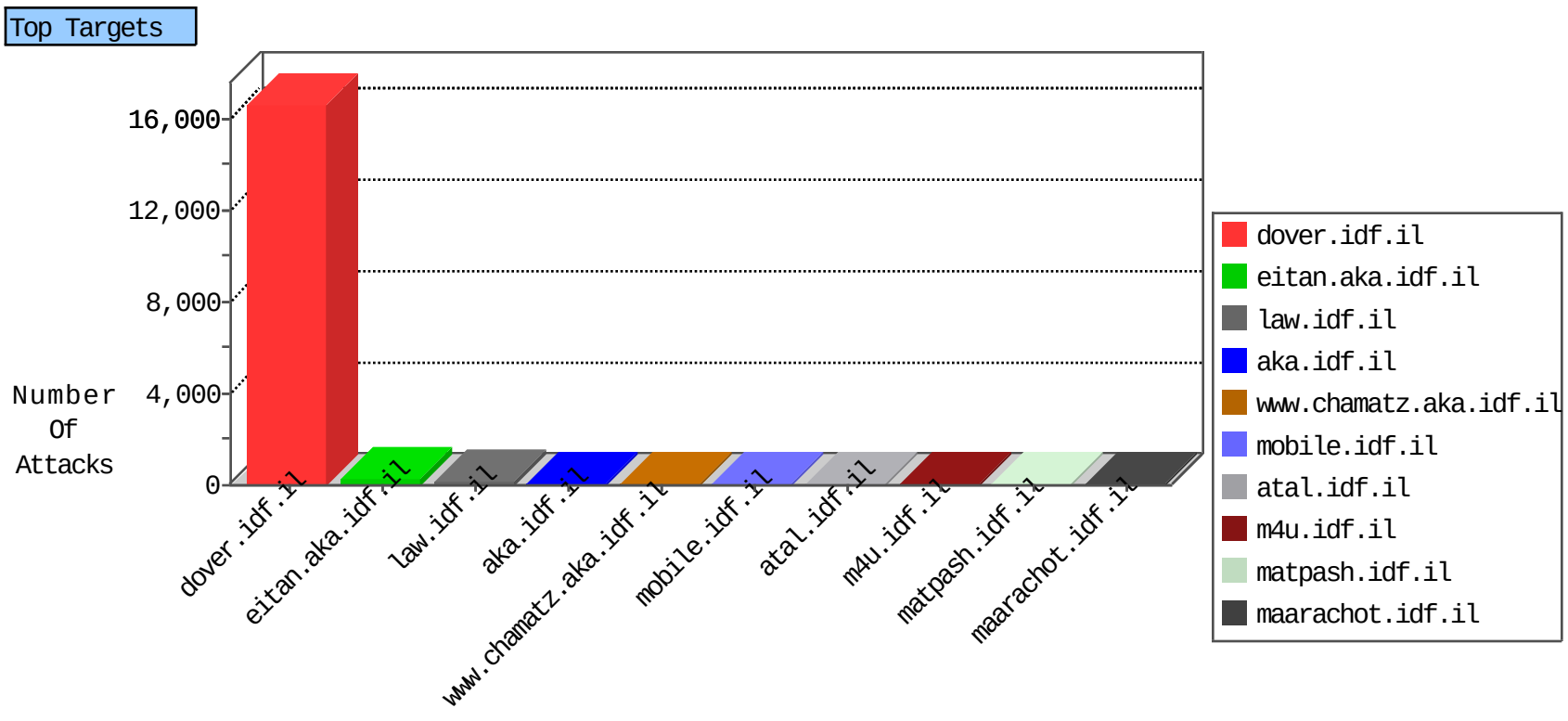
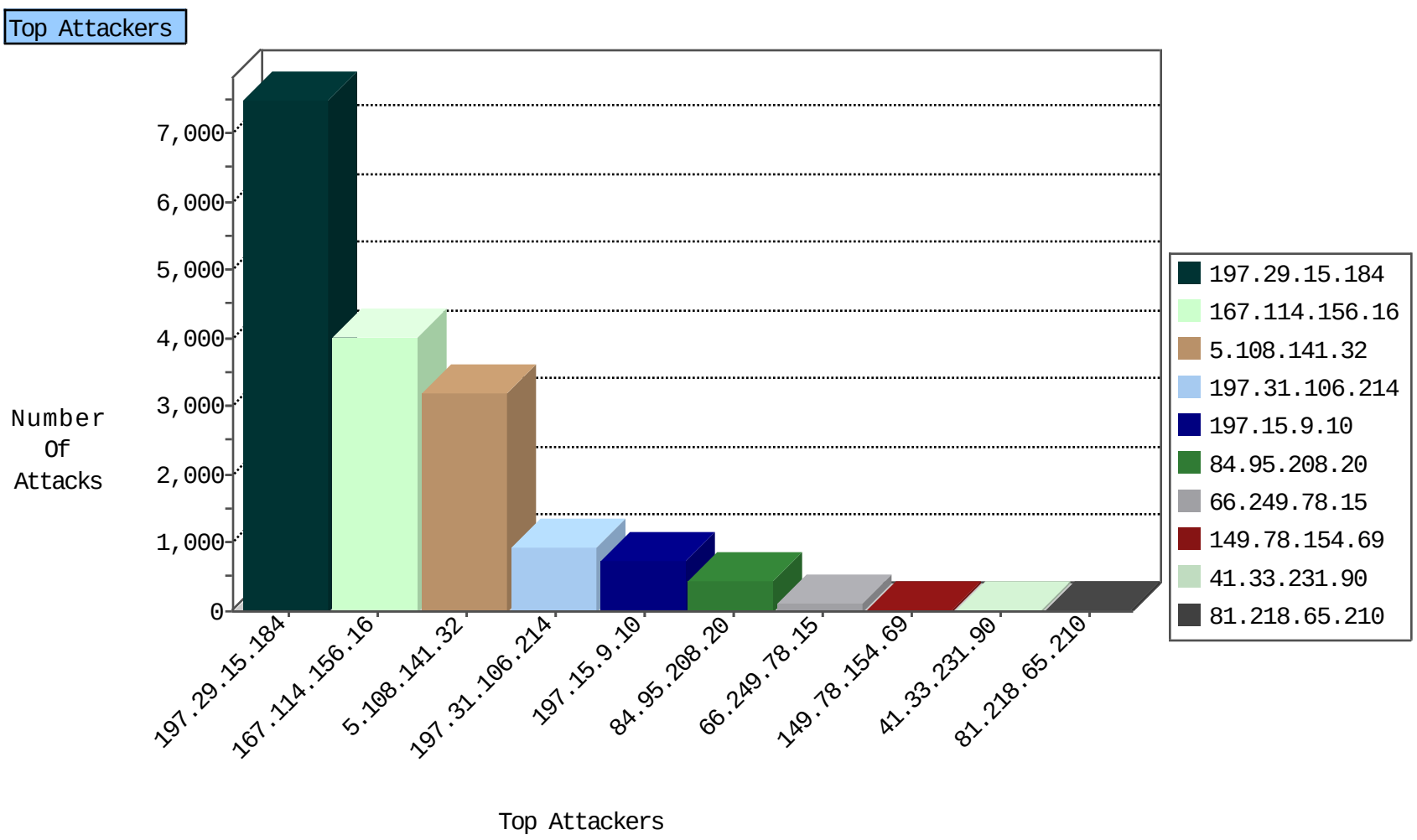
04-10-2016-03:04:01 to 04-10-2016-04:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-03:04:01 to 04-10-2016-04:04:01

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	Block_Ip_Web_In	drop	3978
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3005
109.67.228.35	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2794
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1455
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product3	dest-reset	715
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	713
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	440
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	284
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	79
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	8
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-product2	dest-reset	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	network flood IPv4 TCP-FIN-ACK	drop	2
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	2
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	2
184.105.247.194	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.75	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.84	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
188.138.1.218	Germany	147.237.8.24	e.lifestyle.idf.	Block_Udp_All_Nets	drop	1
42.112.10.80	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
172.58.224.78	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
42.112.10.85	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.81	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
184.105.139.110	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.87	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1
42.112.10.65	Vietnam	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.83	Vietnam	147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	1

04-10-2016-03:04:01 to 04-10-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
144.76.12.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
89.163.148.58	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-03:04:01 to 04-10-2016-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.15	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	116
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
208.100.26.228	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
162.248.100.195	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.77.91.113	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

04-10-2016-03:04:01 to 04-10-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5906
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1314
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	556
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		reject	279
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	215
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	197
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack		reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.154.149.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.65.199.133	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
91.200.12.114	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.242.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.114	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
37.26.148.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.154.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
60.211.5.20	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
197.31.106.214	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.119	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
197.15.9.10	Tunisia	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
40.77.167.86	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
151.80.31.155	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
81.218.154.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
85.65.199.133	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
110.53.183.62	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
197.15.9.10	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
83.170.111.152	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.121.214.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.205	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
185.77.91.113	Turkey	147.237.77.121	e.navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

04-10-2016-03:04:01 to 04-10-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	94
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	15
66.220.145.246	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
5.102.242.86	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.102.242.86	Block	5
66.220.145.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
5.102.242.86	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
66.220.145.245	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
5.102.242.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.220.145.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
198.58.103.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
114.108.214.78	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
31.154.149.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
121.54.54.57	Philippines	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
40.77.167.105	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
156.208.71.26	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.24.139.226	United Kingdom	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
157.55.39.250	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/html/8.asp	Block	1
105.106.3.106	Algeria	147.237.77.216	dover.idf.il	Illegal URL Path Encoding www.idf.il/ar/27%	Block	1
82.24.139.226	United Kingdom	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in www.tikshuv.idf.il/site/general.aspx	Block	1

04-10-2016-03:04:01 to 04-10-2016-04:04:01