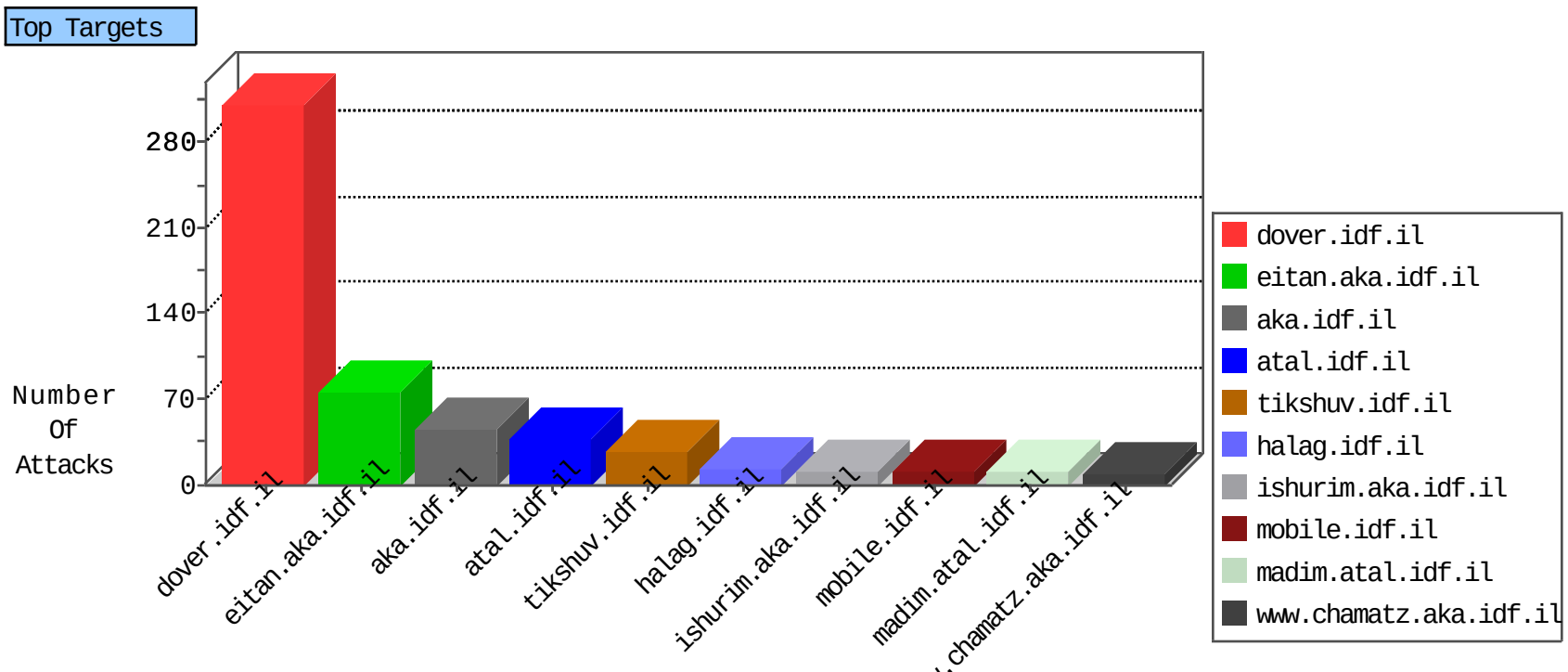
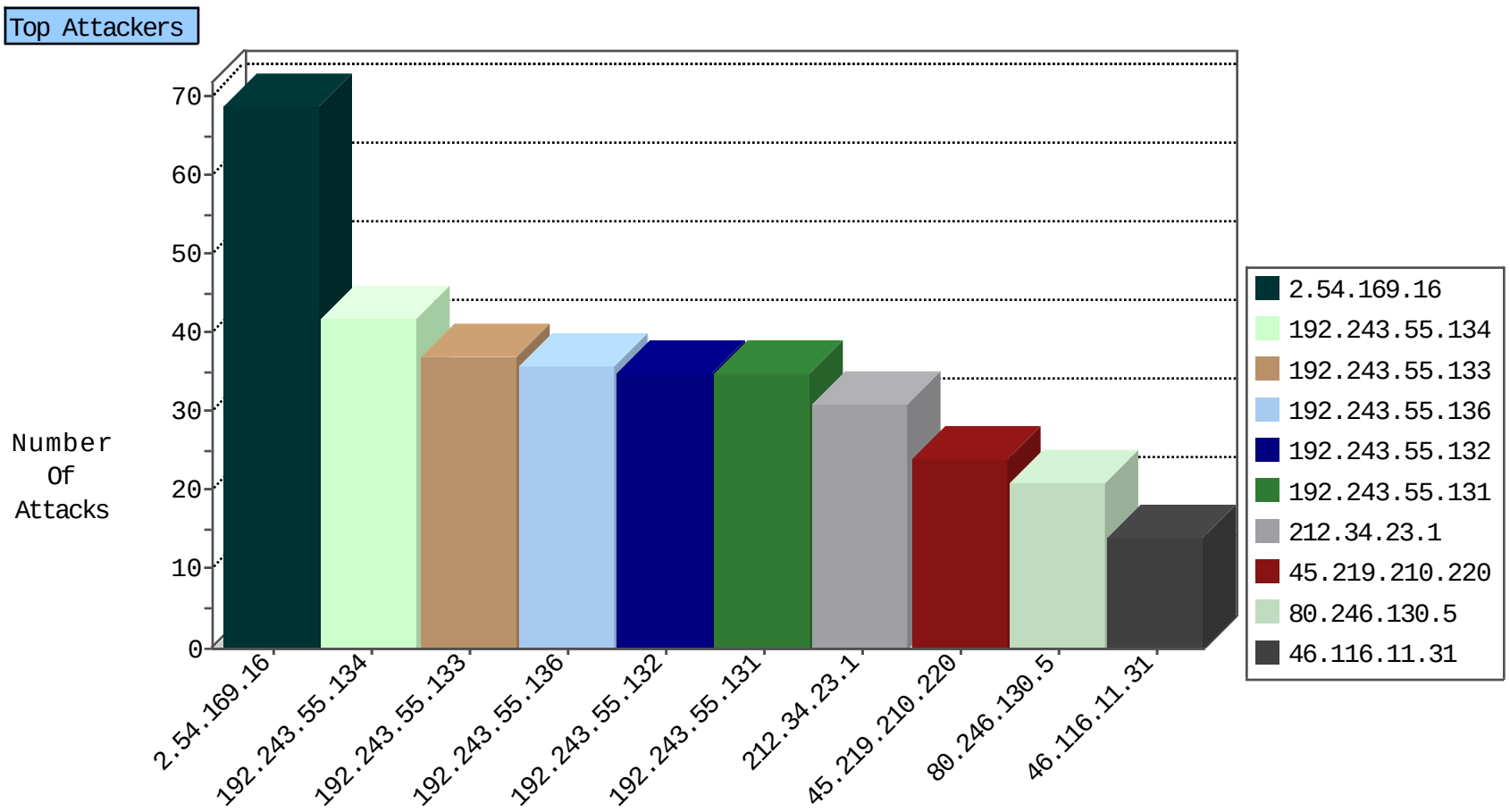
03-04-2016-23:04:07 to 03-05-2016-00:04:07

IDF Under Attack Daily Report



Top Target



Top Attackers

03-04-2016-23:04:07 to 03-05-2016-00:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
183.68.161.220	China	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.75	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.84	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
42.112.10.80	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.73	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.81	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.83	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1

03-04-2016-23:04:07 to 03-05-2016-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.11.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
79.182.151.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
123.126.113.162	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
151.80.31.154	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.153	Italy	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-04-2016-23:04:07 to 03-05-2016-00:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.5	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
66.249.64.153	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.130.5.98	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
95.130.13.220	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
217.10.46.148	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
213.136.91.26	147.237.77.212	Germany	e.dover.idf.il	ET SCAN Potential SSH Scan	1
201.232.25.160	147.237.72.14	Colombia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
191.34.237.213	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.130.13.220	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
82.166.184.187	147.237.8.24	Israel	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
217.10.46.148	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
217.10.46.148	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
201.232.25.160	147.237.72.14	Colombia	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1

03-04-2016-23:04:07 to 03-05-2016-00:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.169.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
37.142.68.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
80.246.130.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
45.219.210.220	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.65.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.67.14.162	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
45.219.210.220	Uruguay	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Block HTTP Non Compliant		monitor	5
46.19.85.225	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
45.219.210.220	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.225	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
65.55.210.159	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
45.219.210.220	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
45.219.210.220	Uruguay	147.237.77.216	dover.idf.il	SYN Attack		reject	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.241	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.32.179.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.78.26.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.22.131.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
132.66.237.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.117.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-04-2016-23:04:07 to 03-05-2016-00:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.23.1	Block	6
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.23.1	Block	6
85.64.134.175	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	4
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 212.34.23.1	Block	3
79.182.189.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.64.134.175	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.64.134.175	Block	3
79.176.241.211	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.mag.idf.il/1117-he/patzar.aspx	Block	2
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.113.89	Block	2
109.253.139.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.23.1	Block	2
121.205.231.151	China	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
121.205.231.151	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/894-he/atal.aspx/xmlrpc.php	Block	1
40.77.167.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method /NavMenu.css.aspx?lang=ar in URL www.idf.ilhttp/1.1	Block	1
86.99.44.112	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.69.89	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
130.193.51.62	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.225	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.97	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
2.52.189.239	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1225-	Block	1
46.19.86.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
121.205.231.151	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 121.205.231.151	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9234-he/refuah.aspx	Block	1
2.54.136.1	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
198.199.84.198	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
66.249.66.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
212.34.23.1	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
37.238.164.57	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
199.87.224.66	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
86.99.44.112	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.69.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1243-he/atal.aspx	Block	1

03-04-2016-23:04:07 to 03-05-2016-00:04:07