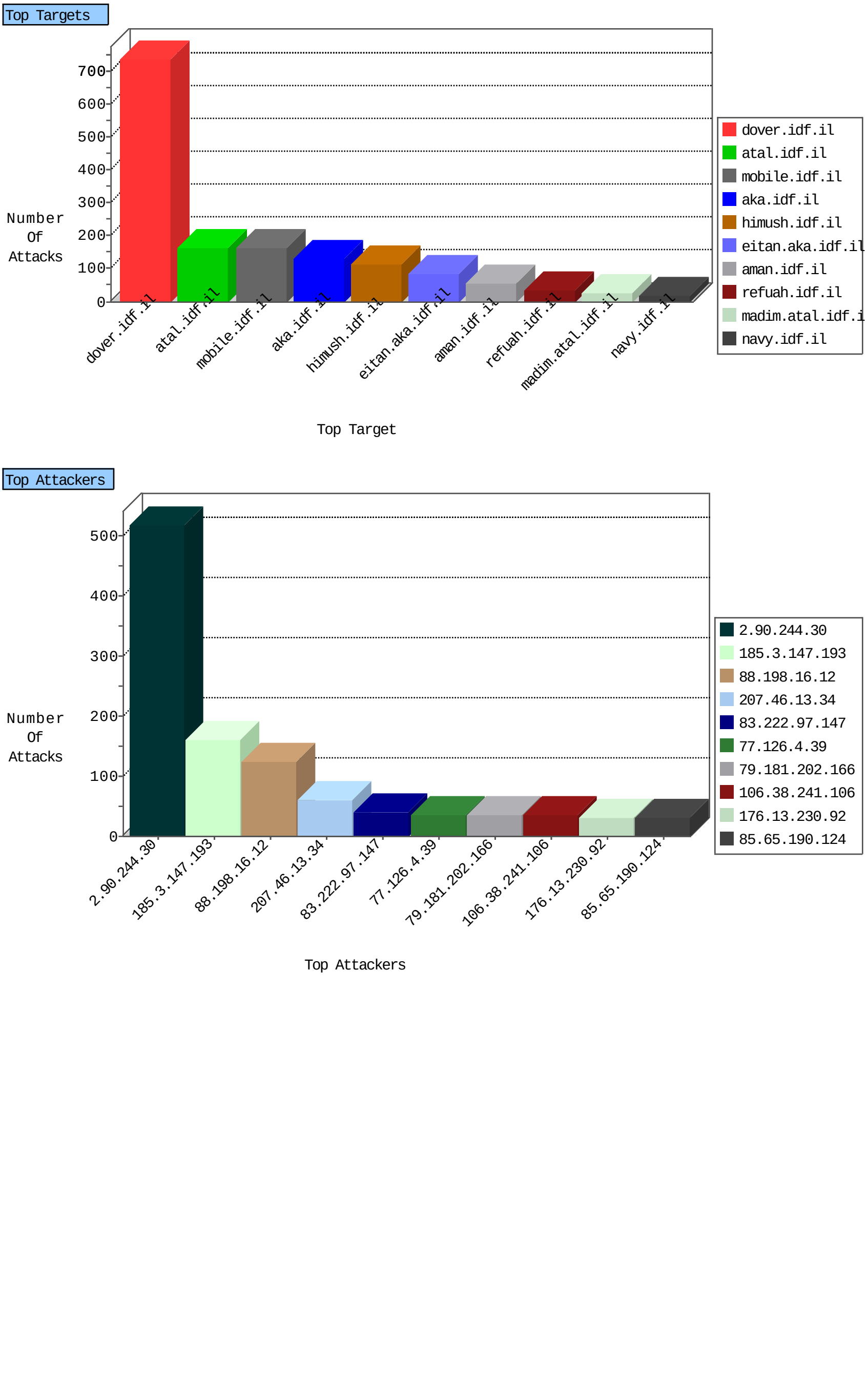
10-03-2016-19:04:07 to 10-03-2016-20:04:07

IDF Under Attack Daily Report



10-03-2016-19:04:07 to 10-03-2016-20:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.216.40	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.30	himush.idf.il	Black List	drop	1

10-03-2016-19:04:07 to 10-03-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.198.16.12	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	82
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	34
88.198.16.12	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	31
88.198.16.12	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	6
88.198.16.12	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
88.198.16.12	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

10-03-2016-19:04:07 to 10-03-2016-20:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
162.250.190.142	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	2
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.208.72.234	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.41.78.139	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 2048	1
88.150.242.119	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sA (2)	1
66.102.9.145	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
222.187.220.241	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
222.187.220.241	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -f -sS	1
66.249.88.17	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
50.254.111.193	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
222.187.220.241	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

10-03-2016-19:04:07 to 10-03-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	505
185.3.147.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	154
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	61
77.126.4.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.181.202.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.230.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.189.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
2.53.55.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.199.133.249	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
176.13.240.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
83.222.97.147	Russian Federation	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
46.19.85.26	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
83.222.97.147	Russian Federation	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
83.222.97.147	Russian Federation	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.32.179.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.202.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
83.222.97.147	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.174.52.3	Russian Federation	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.19.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
75.146.254.30	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
46.19.85.26	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.174.52.3	Russian Federation	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
77.125.47.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.174.52.3	Russian Federation	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
64.94.101.82	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	5
77.125.47.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
64.94.101.82	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
109.253.157.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
199.30.25.67	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
64.94.101.82	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.177	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
64.94.101.82	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.174.52.3	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
188.53.194.168	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
83.222.97.147	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
64.94.101.82	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.18.19.133	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.149.161	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.180.250.83	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
81.218.203.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
177.23.177.146	Brazil	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
185.3.147.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.176.97.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
79.176.97.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

10-03-2016-19:04:07 to 10-03-2016-20:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.190.124	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	31
185.32.179.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
82.80.249.143	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 82.80.249.143	Block	5
79.181.202.166	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
2.53.55.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
77.138.151.228	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	4
84.109.105.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.117.107.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/t	Block	2
89.237.71.85	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
52.1.11.160	United States	147.237.77.170	maarachot.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
82.80.230.228	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 82.80.230.228	Block	1
66.249.76.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/57978.pdf.2005	Block	1
85.65.6.20	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.139.201.66	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
52.5.98.73	United States	147.237.77.170	maarachot.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
207.46.13.123	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
79.178.184.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.19	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sidebar/sidebar.js	Block	1
66.249.69.243	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/govermment/pages/parks2.aspx.54	Block	1
82.80.249.143	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/master/gradiantheader.gif	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dover.aspx	Block	1
207.46.13.164	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
89.237.71.85	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
180.76.15.135	China	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.108.88.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
77.138.93.27	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
207.46.13.175	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
47.209.71.114	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
89.237.71.85	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.237.71.85	Block	1
82.80.230.228	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
185.3.147.193	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c... in www.aka.idf.il/miluim/templates/inner.asp	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1

10-03-2016-19:04:07 to 10-03-2016-20:04:07