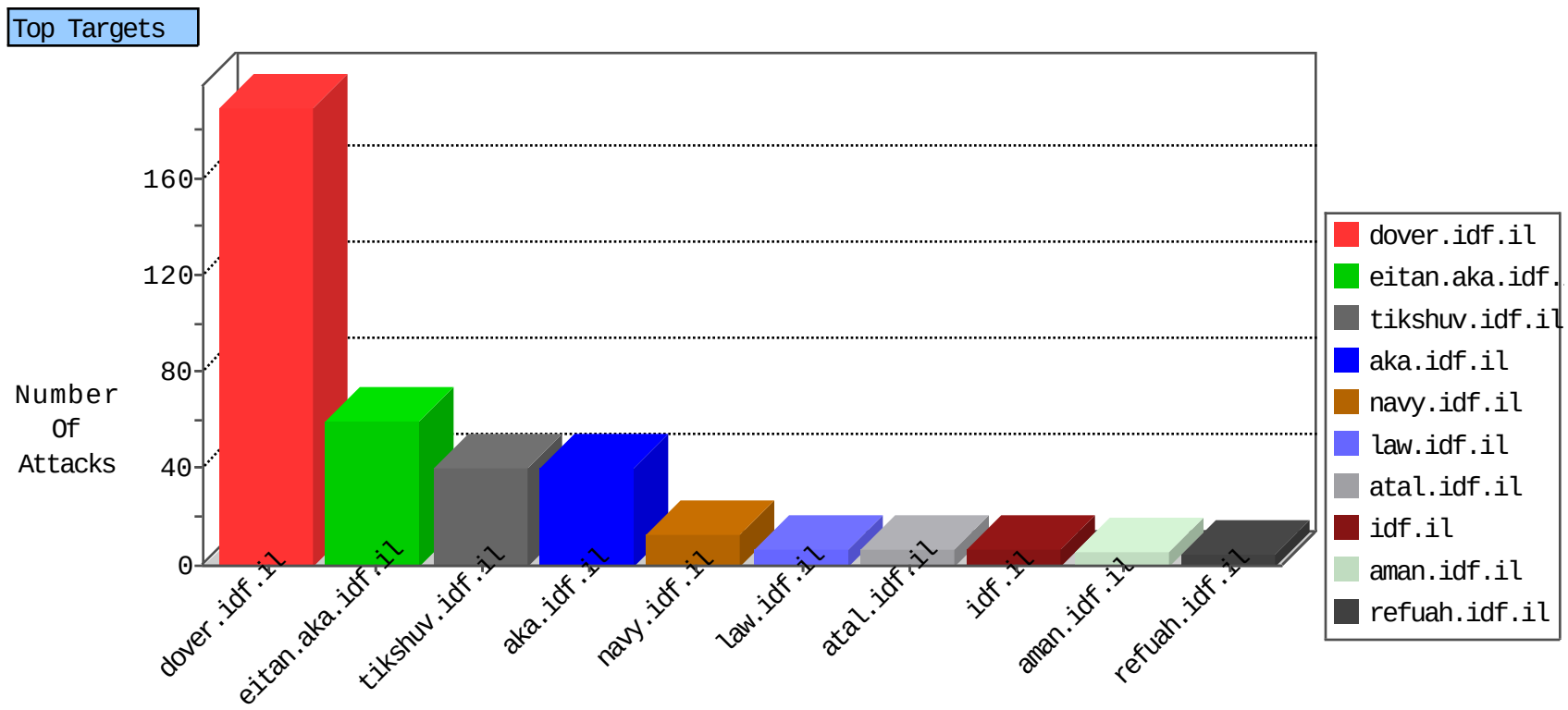
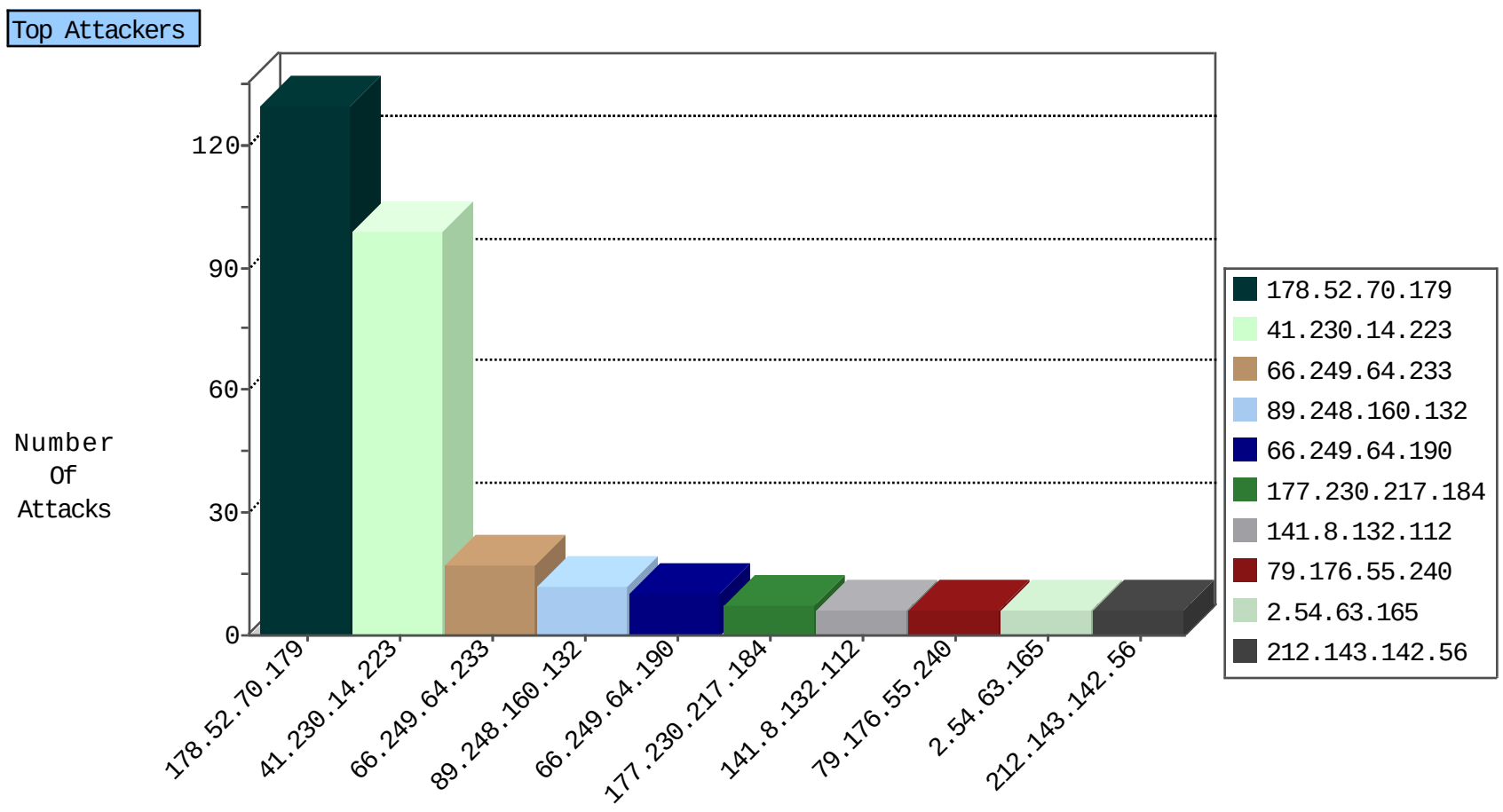
03-06-2016-05:04:04 to 03-06-2016-06:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-06-2016-05:04:04 to 03-06-2016-06:04:04

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
134.147.203.115	Germany	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	2
74.82.47.54	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.120	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.88	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.80	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.88	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.84	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1

03-06-2016-05:04:04 to 03-06-2016-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.191.232.70	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
134.191.232.69	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-06-2016-05:04:04 to 03-06-2016-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.192.0.19	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.103.148.99	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.83.163.128	147.237.76.198	France	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
194.187.249.70	147.237.0.200	Europe	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.20	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.45.210.69	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
94.103.148.99	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
1.34.53.121	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.76.90.223	147.237.76.42	China	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.192.0.20	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

03-06-2016-05:04:04 to 03-06-2016-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.52.70.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	65
178.52.70.179	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	65
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
2.54.63.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.22.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.130.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
177.230.217.184	Mexico	147.237.0.33	idf.il	drop		drop	2
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
177.230.217.184	Mexico	147.237.0.35	akaws.idf.il	drop		drop	2
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
37.46.41.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
114.109.243.129	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.91	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.137.209.205	Ukraine	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
89.248.160.132	Netherlands	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.107	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.160.132	Netherlands	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
52.28.32.164	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
89.248.160.132	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.83	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.125.2.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
182.50.130.133	Singapore	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
52.28.32.164	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
216.218.206.120	United States	147.237.0.33	idf.il	drop		drop	1
89.248.160.132	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.46.13.62	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
89.248.160.132	Netherlands	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.88	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.139.157.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.115	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
52.28.32.164	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.22.131.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
89.248.160.132	Netherlands	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.14	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
89.248.160.132	Netherlands	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.88	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
89.248.160.132	Netherlands	147.237.0.33	idf.il	drop		drop	1
184.105.247.243	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.28.32.164	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

03-06-2016-05:04:04 to 03-06-2016-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	17
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	7
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	6
79.176.55.240	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	3
79.176.55.240	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	2
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 41.230.14.223	Block	2
17.142.159.148	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	2
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.en/error.png)	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1001-en/eitan.aspx	None	1
198.71.226.42	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
134.0.11.15	Spain	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/test/wp-admin/	Block	1
24.184.188.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.66.64	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1130-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
217.118.78.94	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter l	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1086-en/eitan.aspx	None	1
177.230.217.184	Mexico	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
103.41.177.26		147.237.76.86	navy.idf.il	Abnormally Long Request request version	Block	1
50.177.155.231	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1002-en/eitan.aspx	None	1
207.241.229.151	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan/pratim/pirteykatava	Block	1
149.78.182.199	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
24.215.169.59	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.125	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1074-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1149-en/eitan.aspx	None	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/opcemetery/opcemetery.aspx	Block	1
188.165.204.224	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
103.41.177.26		147.237.76.86	navy.idf.il	Illegal HTTP Version instanceof HTMLElement	Block	1
62.210.178.179	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
213.8.204.24	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1028-en/eitan.aspx	None	1
149.78.248.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
40.77.167.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/999-en/eitan.aspx	None	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
197.35.225.175	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
103.41.177.26		147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/).html(	Block	1
213.8.204.24	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.8.204.24	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1084-en/eitan.aspx	None	1
177.230.217.184	Mexico	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /tmunblock.cgi	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
197.35.225.175	Egypt	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
113.76.90.223	China	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
217.118.78.94	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter f	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1085-en/eitan.aspx	None	1
177.230.217.184	Mexico	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/news/news.in.aspx	Block	1

03-06-2016-05:04:04 to 03-06-2016-06:04:04