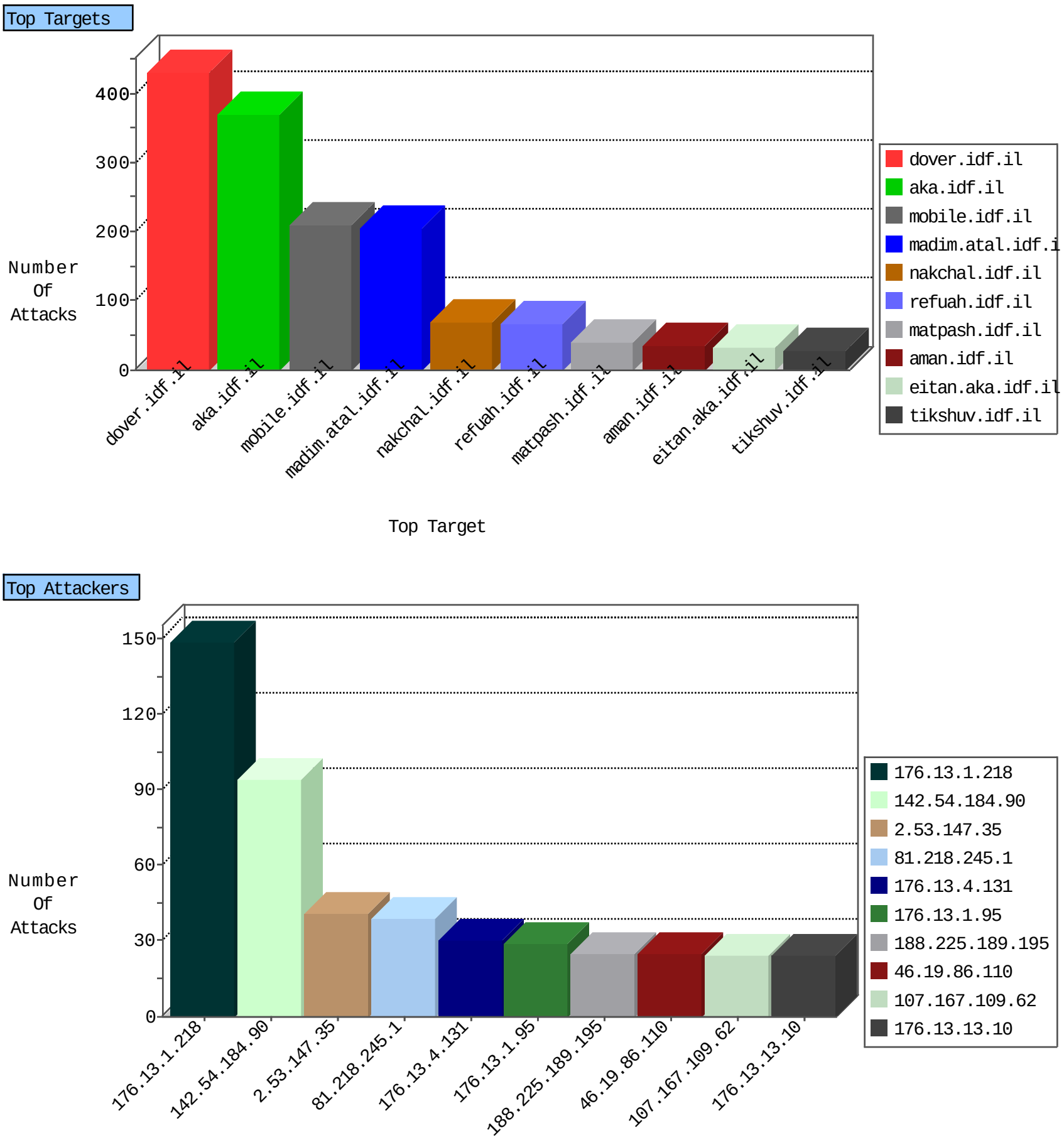
09-29-2016-17:04:08 to 09-29-2016-18:04:08

IDF Under Attack Daily Report



09-29-2016-17:04:08 to 09-29-2016-18:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.183	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
63.141.231.197	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
198.204.247.222	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
142.54.180.68	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
198.204.247.222	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
185.3.147.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
63.141.231.194	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
63.141.231.195	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.198.11	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
63.141.250.157	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
198.204.255.75	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
192.187.101.237	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	1
125.107.240.140	China	147.237.76.30	himush.idf.il	Black List	drop	1
173.208.207.134	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
69.30.193.253	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
204.12.217.5	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
192.187.101.238	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
63.141.231.211	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
69.30.227.218	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
192.187.118.20	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
173.208.150.118	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
63.141.231.213	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
198.204.255.74	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
192.69.89.173	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
192.187.118.69	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1

09-29-2016-17:04:08 to 09-29-2016-18:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.54.184.90	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	94
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-29-2016-17:04:08 to 09-29-2016-18:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.201.60	147.237.77.243	Israel	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	10
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.228.59.47	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 2048	1
141.226.161.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.245.1	147.237.76.31	Israel	nakchal.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
109.228.59.47	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
109.228.59.47	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
65.183.101.8	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.72.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.228.59.47	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.129.160.229	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
2.53.166.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.228.59.47	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.106	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
163.172.129.15	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 4096	1
146.200.148.0	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -f -sS	1
77.127.72.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.228.59.47	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
65.183.101.8	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
109.228.59.47	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
65.183.101.8	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
109.228.59.47	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.112.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.228.59.47	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.129.160.229	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
109.228.59.47	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-29-2016-17:04:08 to 09-29-2016-18:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.4.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
107.167.109.62	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
176.13.13.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.110	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	23
109.253.137.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.76.212.177	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
188.73.193.175	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
188.225.189.195	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.53	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.102.196.180	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	15
2.53.147.35	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
192.115.29.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
79.177.202.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
176.13.228.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
37.26.149.167	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
109.253.201.60	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	10
2.53.147.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
31.154.81.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.152	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.228	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.152	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.179.117.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.147.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
2.53.147.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
66.102.6.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
194.9.252.237	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.228	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
109.64.99.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.156.172.87	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.117.16.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.249	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
176.13.251.70	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.117.16.235	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.120.154.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.139.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.85.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.12.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.136.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.71.242.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.17.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5

09-29-2016-17:04:08 to 09-29-2016-18:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	140
176.13.1.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
81.218.245.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	22
60.163.56.240	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 60.163.56.240	Block	17
81.218.245.1	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 81.218.245.1	Block	14
80.246.137.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
37.26.147.200	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	8
60.163.56.240	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
37.26.148.249	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	5
176.213.17.10	Russian Federation	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in URL from 176.213.17.10	Block	5
176.213.17.10	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in URL from 176.213.17.10	Block	5
2.55.128.82	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
37.26.148.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	3
87.69.8.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.249.110	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	2
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.10.29	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.26.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.64.17.152	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
141.226.232.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
109.64.173.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.148.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.205.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.115.29.180	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
89.138.112.109	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
80.246.138.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.1.218	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
77.127.61.54	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/matash	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
109.253.156.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.187	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
82.81.198.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.139.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ò[[#11]]•7K•~ËžÞÝp#012ôjÈó‰b• in URL	Block	1
79.180.22.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
217.132.117.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl33 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
134.17.31.249	Belarus	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
93.172.99.217	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
2.55.159.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.2.90	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.84.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name ¿"$wéD[[#15]]q	Block	1
109.253.197.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
60.163.56.240	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
212.29.220.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.102.169.113	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	1

09-29-2016-17:04:08 to 09-29-2016-18:04:08