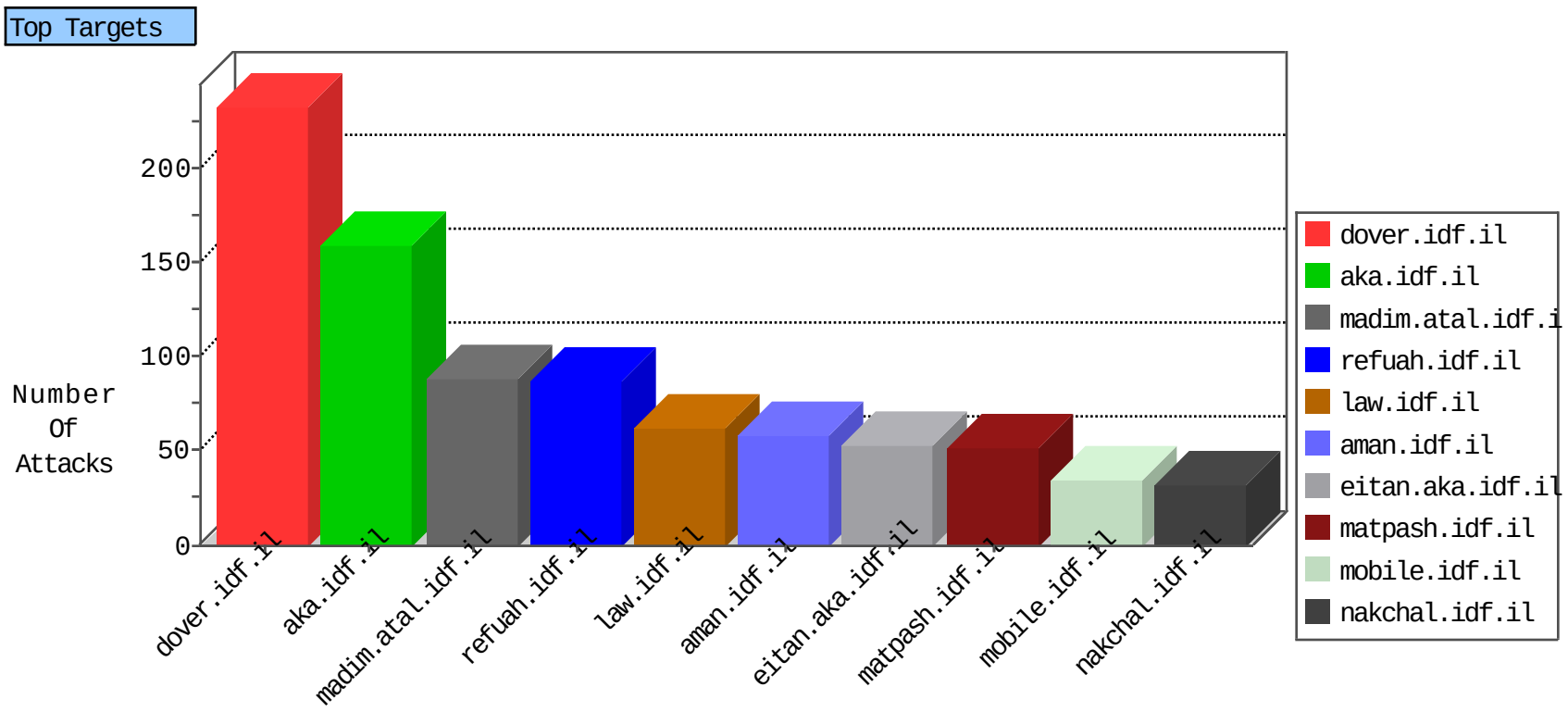
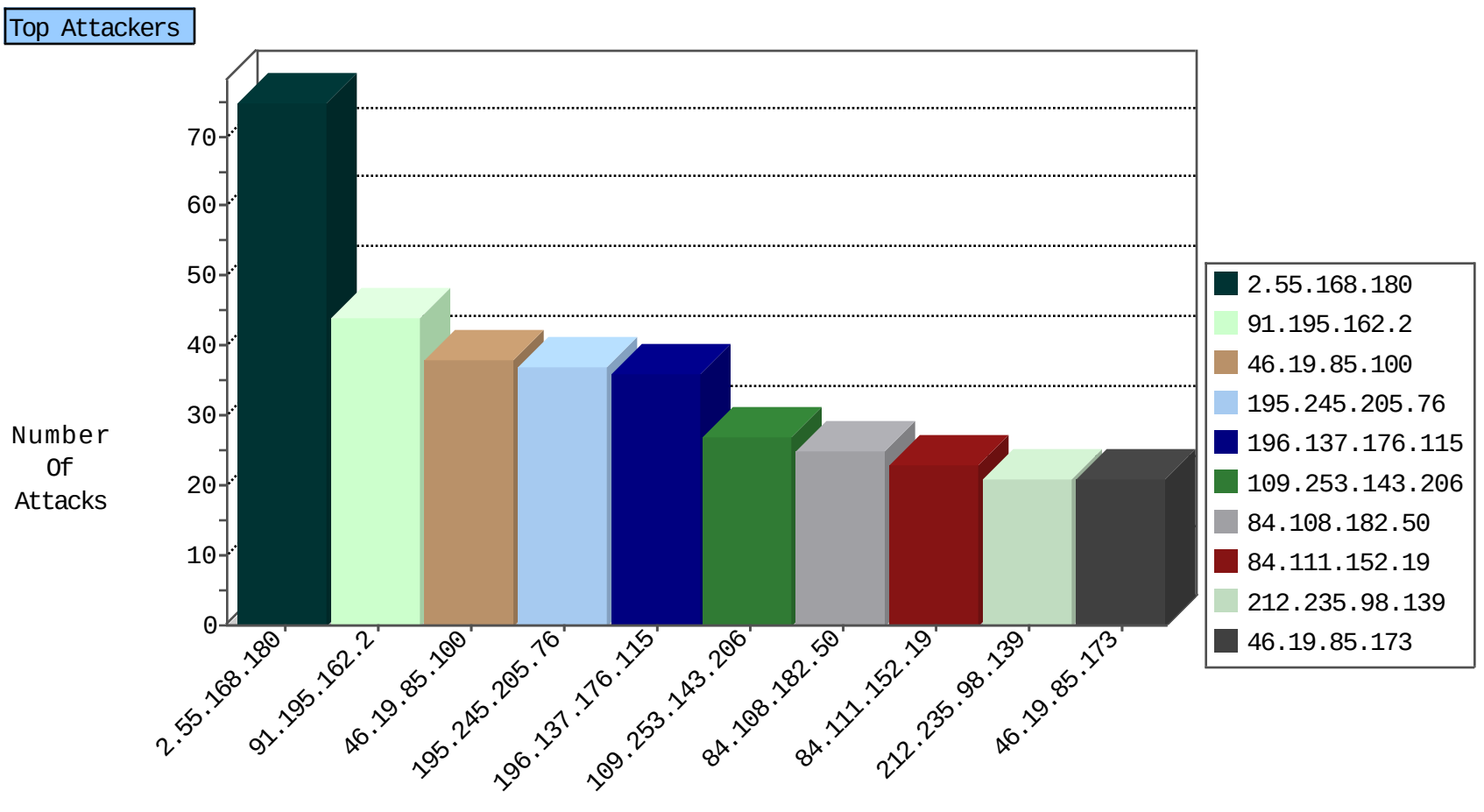
09-05-2016-14:04:01 to 09-05-2016-15:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-05-2016-14:04:01 to 09-05-2016-15:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.180.6	United States	147.237.77.74	law.idf.il	TCP Scan (vertical)	drop	168
109.253.213.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
79.182.117.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.25.74.130	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
217.23.9.123	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
79.177.98.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.53.22.3	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.136.2	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
2.55.182.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-05-2016-14:04:01 to 09-05-2016-15:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.52.175.27	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

09-05-2016-14:04:01 to 09-05-2016-15:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
208.52.175.27	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	11
212.179.223.120	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	8
195.245.205.76	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
195.245.205.76	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.72.217	Russian Federation	e.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.0.33	Russian Federation	idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
195.245.205.76	147.237.76.199	Russian Federation	e.nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
2.53.136.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.76.147	Russian Federation	chinuch.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.77.243	Russian Federation	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
163.172.51.213	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
195.245.205.76	147.237.76.38	Russian Federation	e.e.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.77.227	Russian Federation	e.hamaz.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
94.102.52.71	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.76.31	Russian Federation	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
87.69.6.56	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.205	Russian Federation	prisha.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.72.167	Russian Federation	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
84.109.89.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.176	Russian Federation	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
81.218.80.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.121	Russian Federation	e.navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.8.14	Russian Federation	e.orchot.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
46.19.85.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.61	Russian Federation	e.cogat.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.0.34	Russian Federation	tikshuv.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.76.200	Russian Federation	eitan.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
5.255.90.133	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
208.100.26.228	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
195.245.205.76	147.237.76.196	Russian Federation	e.sviva.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
163.172.51.213	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
195.245.205.76	147.237.76.44	Russian Federation	e.refuah.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.77.235	Russian Federation	sviva.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
162.250.190.142	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	1
195.245.205.76	147.237.76.34	Russian Federation	yohalan.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
91.121.132.153	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
85.65.211.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.178	Russian Federation	e.matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.72.156	Russian Federation	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
82.81.37.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.170	Russian Federation	maarachot.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.8.24	Russian Federation	e.lifestyle.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
79.183.60.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.77.74	Russian Federation	law.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
195.245.205.76	147.237.0.35	Russian Federation	akaws.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
212.199.118.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.245.205.76	147.237.76.201	Russian Federation	e.atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1

09-05-2016-14:04:01 to 09-05-2016-15:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.195.162.2	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
196.137.176.115	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.19.85.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.133.181	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.27	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.55.168.180	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
2.55.168.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.55.168.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
89.139.218.180	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
2.55.168.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
46.19.85.119	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
147.235.8.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
2.55.168.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.146.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.168.180	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.100	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
176.13.225.90	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
147.235.8.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.55.168.180	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.100	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.100	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.215	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.147.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.225.90	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
2.55.168.180	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.225.90	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
147.235.8.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.114	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.133.181	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.177.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
82.80.198.164	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
89.139.218.180	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	4
132.70.66.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.55.168.180	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.53.155.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.119	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.55.168.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
94.254.178.71	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-05-2016-14:04:01 to 09-05-2016-15:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
84.111.152.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.182.50	Block	18
185.32.179.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
91.228.248.251	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	10
132.68.98.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
132.68.98.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 132.68.98.40	Block	6
109.253.195.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
192.116.205.43	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	5
31.168.7.20	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
192.116.205.43	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.116.205.43	Block	4
37.26.149.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
91.228.248.251	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/9/	Block	3
84.111.152.19	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
2.55.181.34	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
212.76.119.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	2
2.53.16.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.249.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
131.253.27.10	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.3.147.246	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 185.3.147.246	Block	2
82.80.193.240	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
23.95.187.221	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/main/	Block	1
176.13.16.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.79.185	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.79.185	Block	1
109.253.215.229	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.86.126	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	1
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
82.81.60.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.81.60.9	Block	1
37.26.146.141	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
132.68.98.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/_vti_bin/owssvr.dll	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1394-he/refuah.aspx	Block	1
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.125.79.185	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
66.249.69.93	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/724-4483-he/patzar.aspx	Block	1
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
212.179.155.129	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
82.81.60.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/karpaz	Block	1
192.115.67.2	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.75	Block	1
2.53.32.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
192.116.205.43	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
84.108.182.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1

09-05-2016-14:04:01 to 09-05-2016-15:04:01