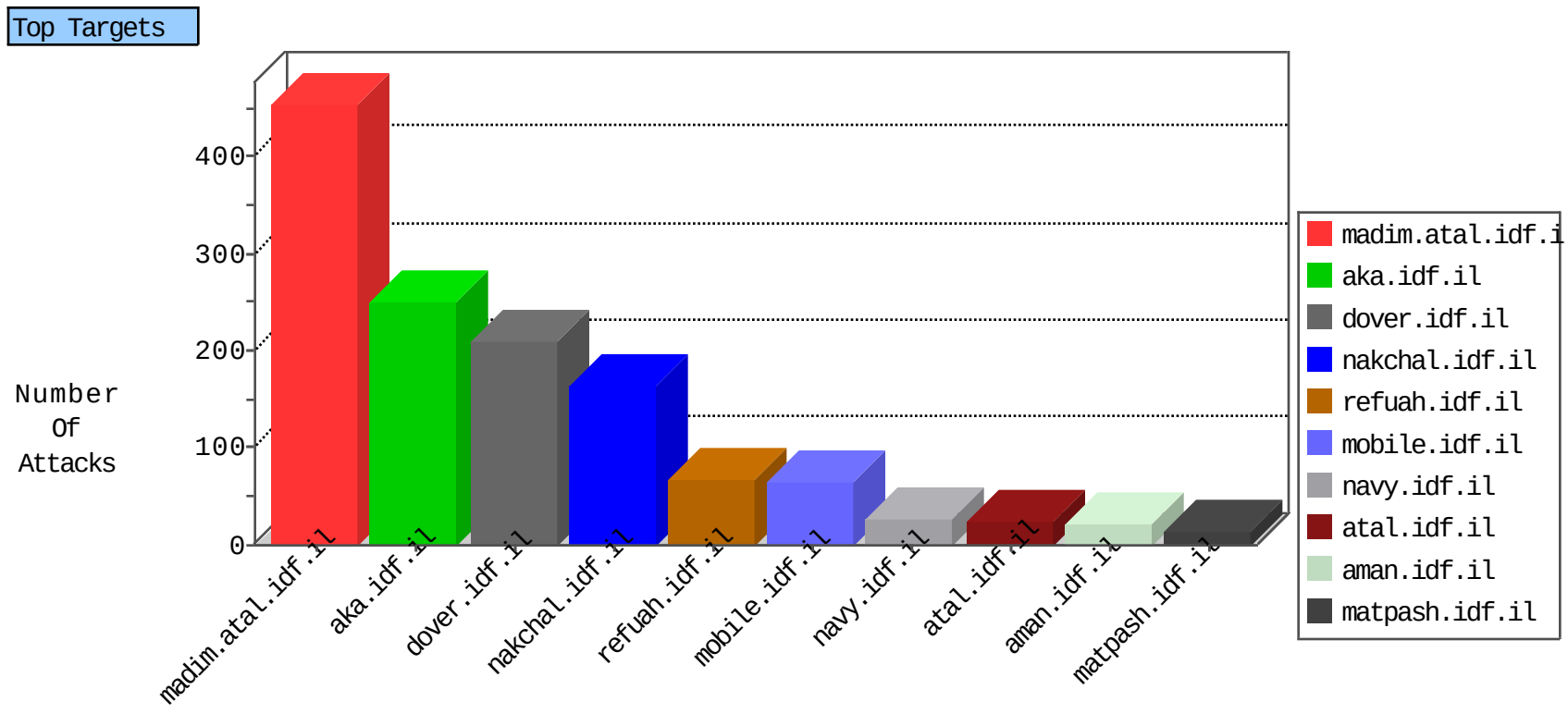
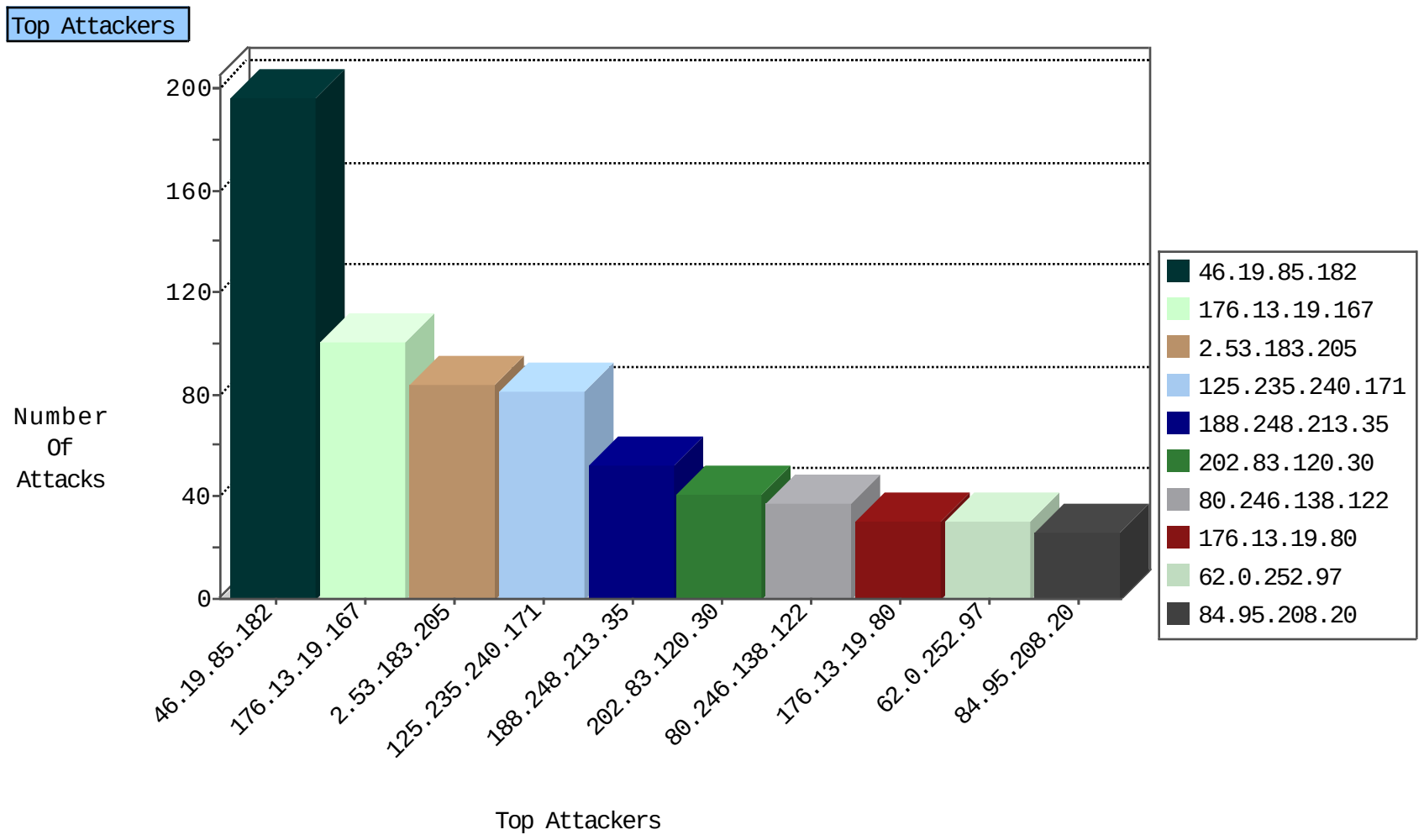
09-28-2016-10:04:03 to 09-28-2016-11:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-28-2016-10:04:03 to 09-28-2016-11:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.94.235	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
192.187.118.67	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
123.249.0.134	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
192.187.101.238	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
192.187.118.21	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1

09-28-2016-10:04:03 to 09-28-2016-11:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-28-2016-10:04:03 to 09-28-2016-11:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.254	147.237.76.31	Israel	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
37.220.31.10	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.76.114	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.181.13.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.91.21	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.155.58.28	147.237.77.61	Indonesia	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.255.108.192	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.14.94.61	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 4096	1
109.65.102.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.164.49	147.237.76.39	Romania	mobile.meitav.idf.i	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.178.187.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.166.162.162	147.237.72.166	Pakistan	aka.idf.il	Xenu Link Sleuth User Agent	1
46.19.85.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
37.220.31.10	147.237.76.176	United Kingdom	test.ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
132.72.86.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.211.102.129	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
109.253.211.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.92.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.168.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-28-2016-10:04:03 to 09-28-2016-11:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
125.235.240.171	Vietnam	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	71
188.248.213.35	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
62.0.252.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
82.166.229.117	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
80.246.138.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
80.246.138.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
62.0.228.129	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
2.53.130.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.34.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
2.53.2.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.138.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.95.131.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
17.78.107.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.120.113.158	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
100.92.64.108		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
188.248.213.35	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.120.113.158	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.62.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.79.17	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.132.136	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.247.181	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
185.32.179.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.6.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
82.166.93.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
199.203.170.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
125.235.240.171	Vietnam	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.254	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.47	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.47	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.49.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.183	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.200.205.66	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4

09-28-2016-10:04:03 to 09-28-2016-11:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	197
176.13.19.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
2.53.183.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
176.13.19.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
109.253.220.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.153.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.248.213.35	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.248.213.35	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
185.32.179.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.102.195	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
2.55.60.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.240.174	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.191.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.125.10	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
141.226.218.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
77.125.45.38	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
82.166.229.117	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
188.248.213.35	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 188.248.213.35	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
109.65.32.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.128.48.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
212.143.103.6	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
185.97.81.93	Ireland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
120.27.37.74	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
85.64.105.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.210.177.43	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.210.177.43	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
176.13.249.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.124.53.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
109.65.138.229	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
62.219.145.163	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/275-he/patzar.aspx	Block	1
212.235.79.14	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
80.246.130.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
87.69.20.111	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.210.177.43	Israel	147.237.76.42	refuah.idf.il	Multiple _vti_ from 46.210.177.43	Block	1
37.26.149.207	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
188.248.213.35	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized Method OPTIONS for 147.237.77.216/	Block	1

09-28-2016-10:04:03 to 09-28-2016-11:04:03