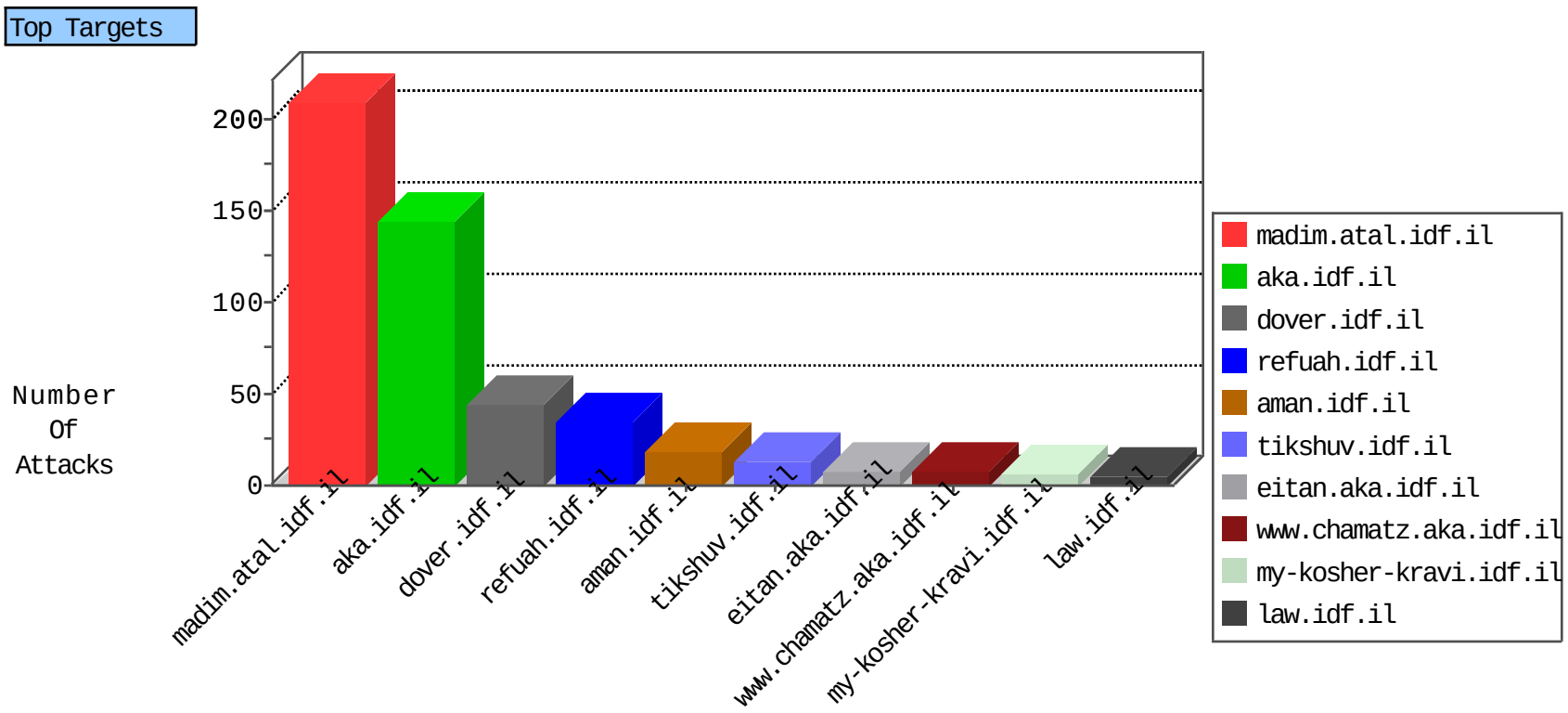
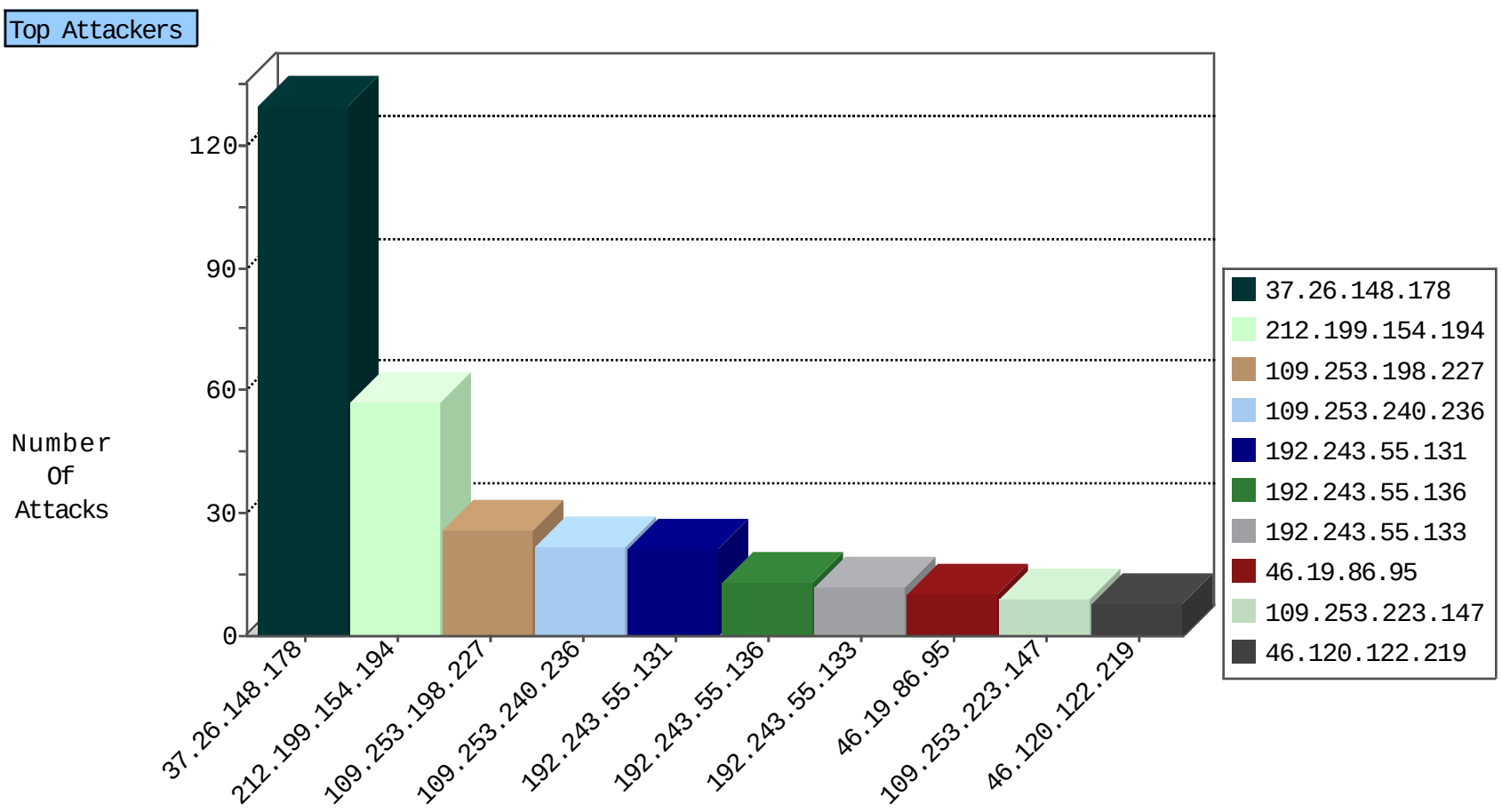
09-12-2016-07:04:00 to 09-12-2016-08:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-12-2016-07:04:00 to 09-12-2016-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.39	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
79.177.96.6	Israel	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-12-2016-07:04:00 to 09-12-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.163.131.57	Ukraine	147.237.77.216	dover.idf.i	26949: HTTP: Drupal RESTWS Module Page Callback Code Injection Vulnerability	Block	1

09-12-2016-07:04:00 to 09-12-2016-08:04:00

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	6
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
45.79.71.122	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
50.84.213.146	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
191.96.249.18	147.237.76.34	Chile	yohalan.idf.il	ET SCAN Potential SSH Scan	1
172.245.173.142	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.121.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.166.249.197	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
50.87.113.190	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
50.84.213.146	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
191.96.249.18	147.237.76.148	Chile	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
49.143.187.187	147.237.77.205	Korea, Republic of	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
172.245.173.142	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.158.185	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
93.174.164.92	147.237.77.121	Romania	e.navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.212.209.243	147.237.77.74	Slovenia	law.idf.il	Xenu Link Sleuth User Agent	1
52.166.249.197	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
52.166.249.197	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
211.141.78.56	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

09-12-2016-07:04:00 to 09-12-2016-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.199.154.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	52
37.26.146.156	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.199.154.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.223.147	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.161.43	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.210	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.229.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.143.150	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.223.147	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.169.7.223	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
46.19.86.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.129.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.4.123.172	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
80.246.139.253	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.61.109.18	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.253	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.4.123.172	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
192.243.55.133	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.53.3.199	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.53.25.221	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
192.243.55.131	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
199.241.27.33	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.115.120.61	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
192.243.55.136	United States	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	2
37.26.148.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
98.169.180.29	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.13.22.192	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
192.243.55.133	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.139.47	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.131	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
2.53.57.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
108.61.152.244	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.131	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
62.219.146.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.23.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
192.243.55.134	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

09-12-2016-07:04:00 to 09-12-2016-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
109.253.198.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
109.253.240.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
37.26.148.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.133.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
109.253.133.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.52.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	2
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
108.66.244.46	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
192.243.55.136	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/shared/usercontrols/headerupper	Block	1
37.26.147.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
80.246.130.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/files	Block	1
2.55.3.221	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar/home	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/gallery/showpicture.asp	Block	1
199.241.27.33	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
136.243.35.38	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
80.246.136.249	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
192.243.55.134	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
82.81.137.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
24.8.4.57	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
68.180.228.109	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
46.4.15.197	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.4.15.197	Block	1
192.243.55.131	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector	Block	1
99.186.121.67	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
31.173.232.250	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/contact	Block	1
109.253.223.147	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.96.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to swpost.apple.com/stats	Block	1

09-12-2016-07:04:00 to 09-12-2016-08:04:00