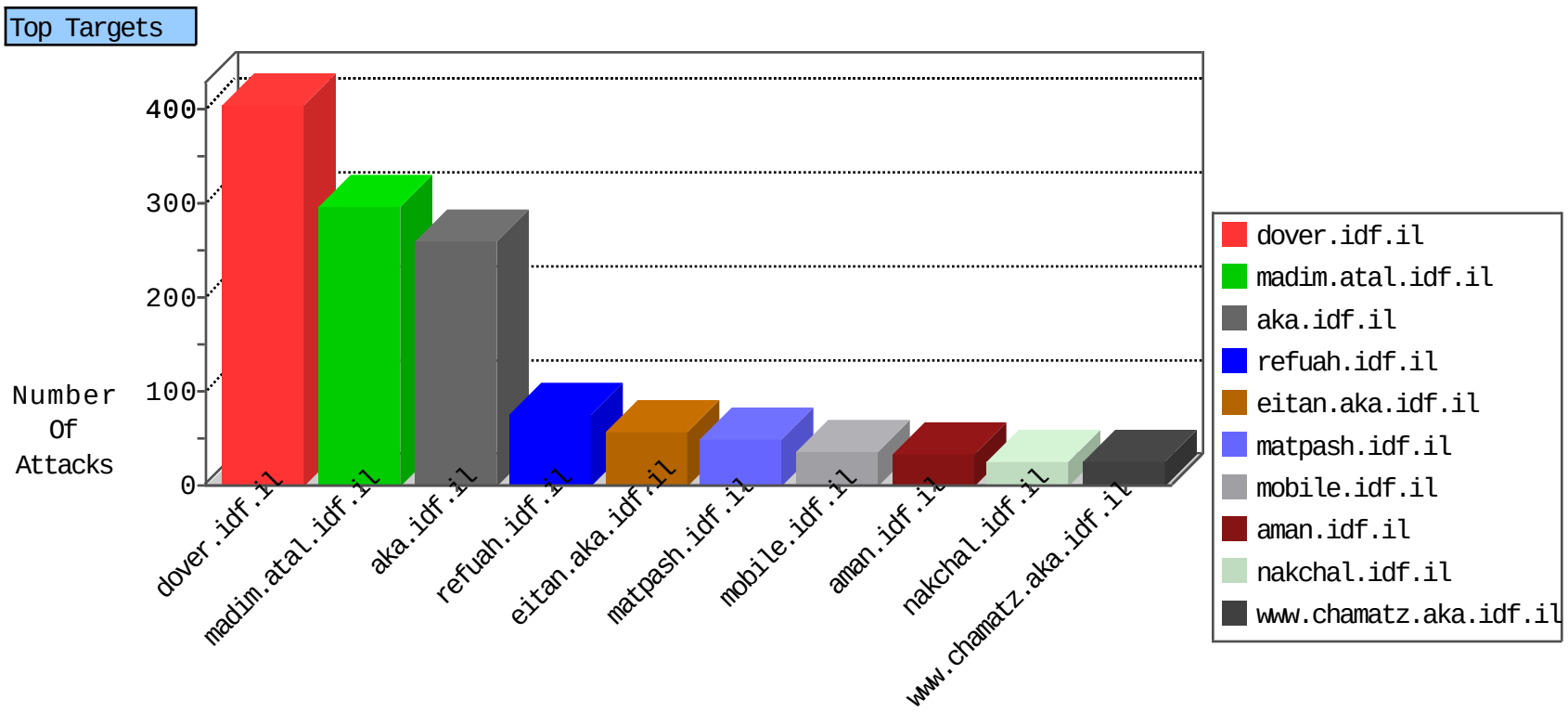
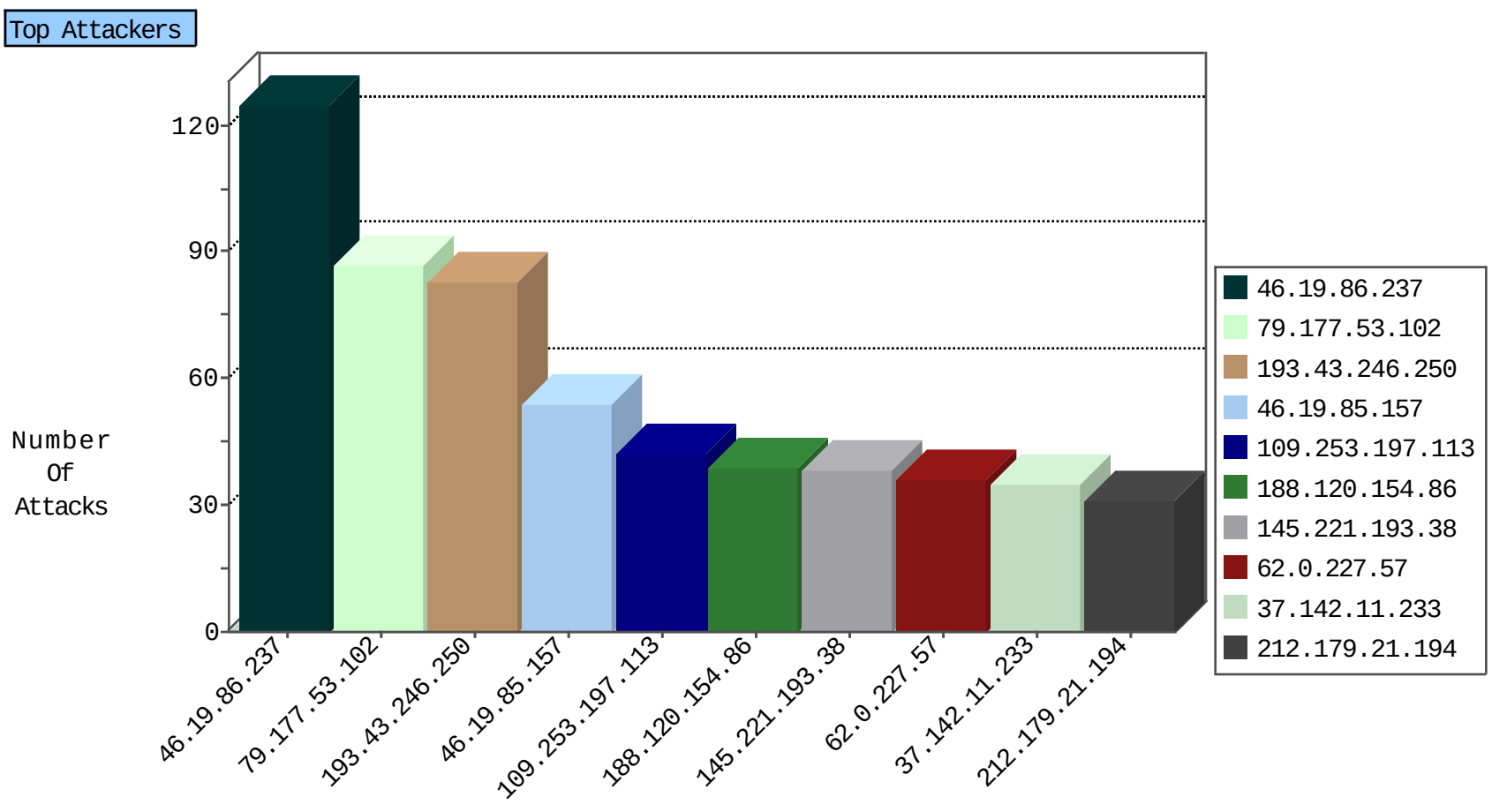
09-13-2016-13:04:04 to 09-13-2016-14:04:04

IDF Under Attack
Daily Report





09-13-2016-13:04:04 to 09-13-2016-14:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.169	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
62.0.98.177	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.117.226.180	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
87.68.59.94	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
195.113.161.83	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	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
10.0.0.1		147.237.72.167	ishurim.aka.idf.il	Black List	drop	1
204.85.191.10	United States	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
131.247.2.241	United States	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
129.93.229.139	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1

09-13-2016-13:04:04 to 09-13-2016-14:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-13-2016-13:04:04 to 09-13-2016-14:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.242.74.253	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
213.231.145.118	147.237.76.86	Bulgaria	navy.idf.il	Xenu Link Sleuth User Agent	1
87.242.74.253	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
213.231.145.118	147.237.72.156	Bulgaria	aman.idf.il	Xenu Link Sleuth User Agent	1
79.179.5.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.231.145.118	147.237.0.15	Bulgaria	kosher-kravi.idf.il	Xenu Link Sleuth User Agent	1
46.120.68.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.255.20.103	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.181.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.234.241.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.253.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.126.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.24.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.147	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
213.231.145.118	147.237.77.74	Bulgaria	law.idf.il	Xenu Link Sleuth User Agent	1
87.242.74.253	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
213.231.145.118	147.237.72.166	Bulgaria	aka.idf.il	Xenu Link Sleuth User Agent	1
81.218.118.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.231.145.118	147.237.0.34	Bulgaria	tikshuv.idf.il	Xenu Link Sleuth User Agent	1
77.125.3.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.40.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.255.20.103	147.237.77.233	United States	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.46.41.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.251.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.120.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.37.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

09-13-2016-13:04:04 to 09-13-2016-14:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
145.221.193.38	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
37.142.11.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
193.43.246.250	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	31
62.0.227.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
188.120.154.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
62.0.212.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
2.55.137.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.145.221.88	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
37.26.146.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
176.13.23.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
62.0.200.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.222.129	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
62.0.247.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
62.0.227.57	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.25	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.136.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.197.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.8.182.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.14.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.253.197.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.253.197.113	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
80.246.136.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.222.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.20.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.197.113	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.179.21.194	Israel	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
80.246.136.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.197.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
130.193.51.3	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
213.8.204.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.55.174.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.55.174.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.104	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.38.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-13-2016-13:04:04 to 09-13-2016-14:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
79.177.53.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
2.53.48.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
80.246.139.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/	Block	15
185.32.179.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.13.14.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
212.179.21.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	8
188.120.154.86	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	8
46.117.158.75	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	8
2.55.28.78	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
176.13.227.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.53.45.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.182.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.102.195.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.148.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method tScripts/Jquery/jquery.nyroModal-1.6.2.js in URL www.refua.atal.idf.ilhttp/1.1	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/bottomcap.gif	Block	1
157.55.39.202	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
46.19.86.104	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Malformed URL get	Block	1
2.55.20.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
92.162.228.170	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
37.26.149.160	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
46.19.86.104	Israel	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 46.19.86.104	Block	1
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Multiple Abnormally Long Request from 46.19.85.69	Block	1
109.253.193.35	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
40.77.167.23	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
77.138.148.106	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
217.132.44.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
46.19.86.104	Israel	147.237.76.31	nakchal.idf.il	Multiple Unknown HTTP Request Method from 46.19.86.104	Block	1
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Multiple Illegal HTTP Version from 46.19.85.69	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	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
52.16.137.212	Ireland	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /	Block	1
212.76.110.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/undefined	Block	1
46.19.86.104	Israel	147.237.76.31	nakchal.idf.il	Abnormally Long Request request version	Block	1
178.199.147.77	Switzerland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
2.53.48.0	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
46.19.86.104	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method 855-M10-D1.xml in URL	Block	1
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 46.19.85.69	Block	1

09-13-2016-13:04:04 to 09-13-2016-14:04:04