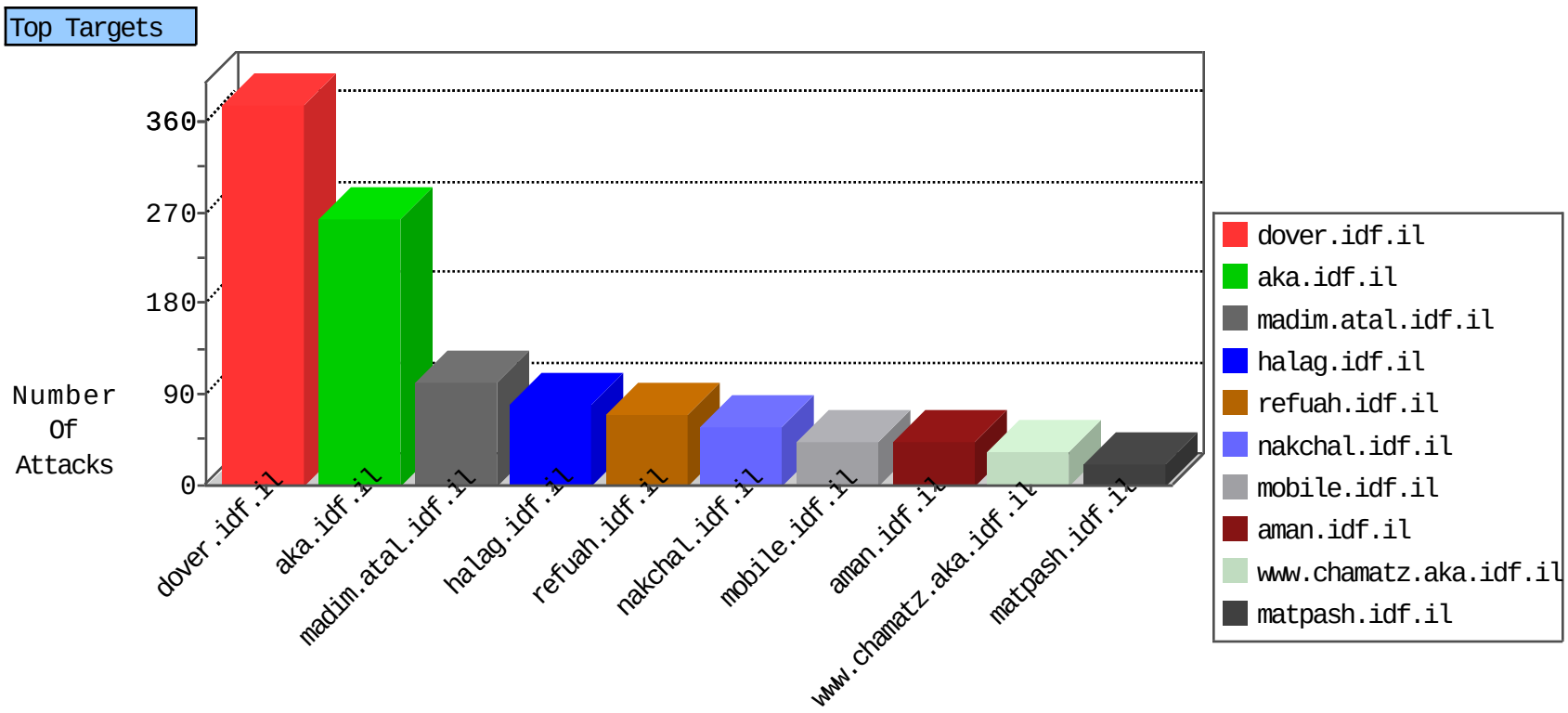
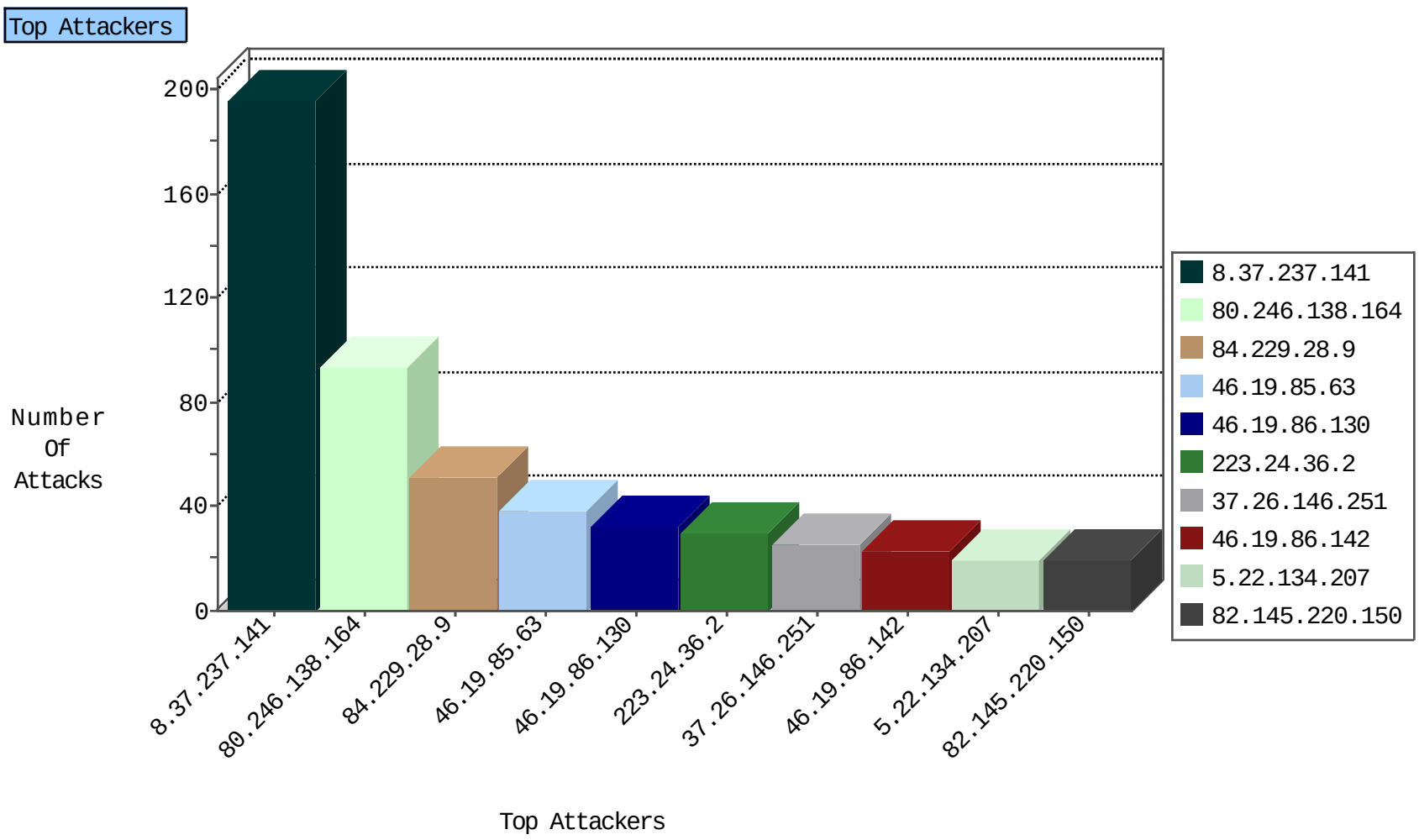
09-26-2016-18:04:08 to 09-26-2016-19:04:08

IDF Under Attack Daily Report





09-26-2016-18:04:08 to 09-26-2016-19:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
79.181.195.175	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.237.141	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
79.178.60.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
186.167.17.116	Venezuela	147.237.8.28	e.mobile-ks.idf.il	L4 Source or Dest Port Zero	drop	3
2.53.8.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.116.40.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.108.91.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
188.138.102.157	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
188.138.102.157	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1
46.116.40.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
209.126.136.2	United States	147.237.76.86	navy.idf.il	Black List	drop	1
188.138.102.157	Germany	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
61.147.110.17	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-26-2016-18:04:08 to 09-26-2016-19:04:08

Top Attackers In IPS

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

09-26-2016-18:04:08 to 09-26-2016-19:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
72.44.88.57	147.237.8.24	United States	e.lifestyle.idf.il	GPL SCAN superscan echo	1
212.116.72.226	147.237.76.148	Sweden	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
211.149.244.79	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
41.215.36.46	147.237.8.46	Kenya	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
185.129.148.230	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.161.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.163.144.203	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.172.103	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.103	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
72.44.88.57	147.237.8.45	United States	e.eitan.idf.il	GPL SCAN superscan echo	1
66.249.93.85	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	1
212.116.72.226	147.237.76.148	Sweden	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.86	United States	navy.idf.il	ET DROP Dshield Block Listed Source	1
37.220.31.10	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.172.103	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.103	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
72.44.88.57	147.237.8.46	United States	e.chinuch.idf.il	GPL SCAN superscan echo	1

09-26-2016-18:04:08 to 09-26-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.237.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	146
84.229.28.9	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
8.37.237.141	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
223.24.36.2	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
37.26.146.251	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.145.220.150	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
107.167.112.131	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
46.19.85.63	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.63	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
176.13.17.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.86.142	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.124.246.133	Lebanon	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.130	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.104	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
93.173.78.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.173	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.104	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
87.69.77.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.238	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.136.247	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.11.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.28.180.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.229.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.142	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
77.124.37.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
77.124.37.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.97.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.142	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.130	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.21.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.181.195.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
141.226.218.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.35	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.32.179.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
87.70.27.28	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.21.108	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
142.54.184.90	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.60.149.68	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.253.218.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

09-26-2016-18:04:08 to 09-26-2016-19:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.138.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
79.176.9.9	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	12
79.181.229.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	5
107.161.12.66	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	4
79.176.9.9	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
207.158.4.66	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	4
109.253.150.175	Israel	147.237.0.19	madim.atal.idf.il	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	2
79.181.198.49	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	2
2.53.20.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.186.40	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	2
109.253.129.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.185.252	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
157.55.39.135	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
37.26.146.251	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
84.102.207.253	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
79.181.112.236	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
77.139.152.86	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/pictures	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
5.22.134.210	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.130.98	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.124.16.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.251	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.19.86.9	Israel	147.237.0.34	tikshuv.idf.il	Distributed Illegal HTTP Version	Block	1
84.229.28.9	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.161.136.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
5.102.242.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.19.100	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
77.138.13.32	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
180.76.15.29	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8905-he/refuah.aspx	Block	1
85.65.112.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
46.19.86.9	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.181.198.49	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1518-he	Block	1
2.53.26.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsList$ctl00$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx	None	1
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
24.141.53.30	Canada	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
79.180.96.201	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
77.138.109.97	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.116.172.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.237.76.204	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
46.19.86.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.146.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.9.9	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.176.9.9	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
157.55.39.60	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
79.180.184.184	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

09-26-2016-18:04:08 to 09-26-2016-19:04:08