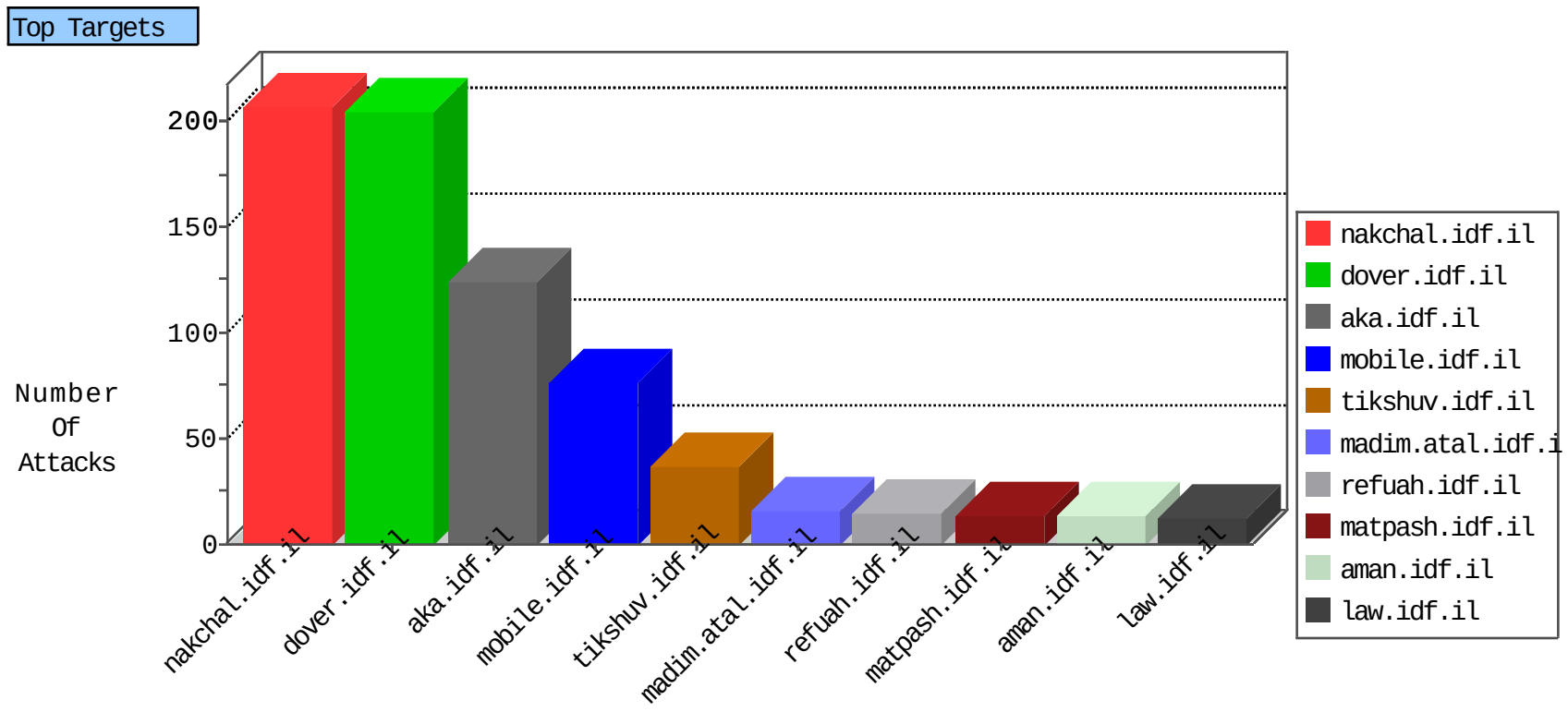
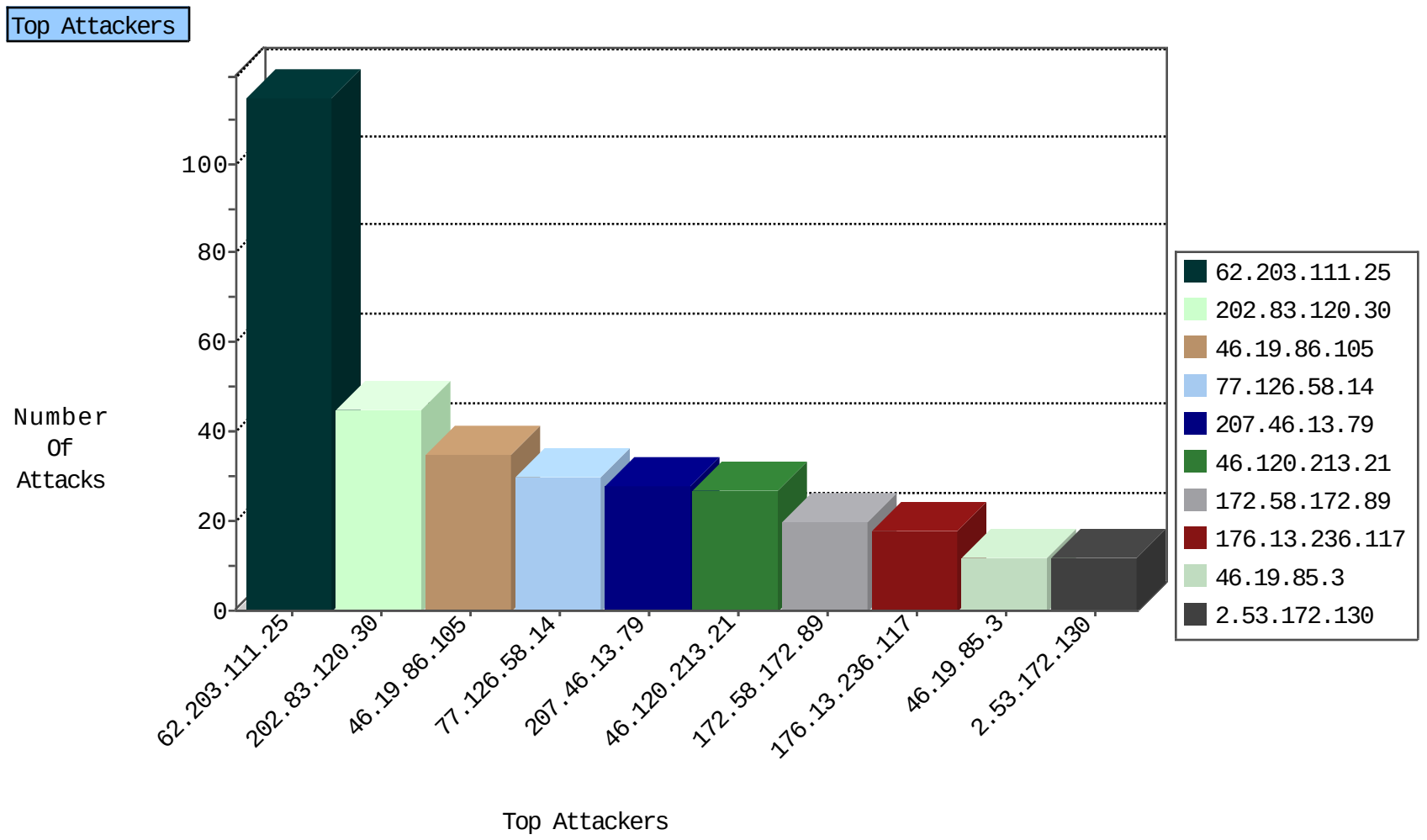
09-28-2016-22:04:03 to 09-28-2016-23:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-28-2016-22:04:03 to 09-28-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.52.10	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
46.120.130.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-28-2016-22:04:03 to 09-28-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
125.208.24.2	China	147.237.77.176	matpash.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-28-2016-22:04:03 to 09-28-2016-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
90.109.12.97	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	2
220.133.108.138	147.237.8.14	Taiwan	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
90.109.12.97	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
90.109.12.97	147.237.0.34	France	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
90.109.12.97	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
154.16.199.242	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
115.74.138.238	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.122.226.88	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
112.217.150.112	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.33	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.221.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.137.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
90.109.12.97	147.237.0.35	France	akaws.idf.il	ET SCAN Potential SSH Scan	1
90.109.12.97	147.237.0.33	France	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
176.13.226.107	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
61.240.144.65	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
121.41.88.64	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
59.122.226.88	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
112.217.150.112	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Potential SSH Scan	1
54.144.119.103	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
112.217.150.112	147.237.0.15	Korea, Republic of	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
40.114.15.49	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

09-28-2016-22:04:03 to 09-28-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
207.46.13.79	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	28
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	25
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	23
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	23
46.19.86.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
95.85.26.101	Netherlands	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
2.53.172.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
172.58.172.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
95.85.26.75	Netherlands	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.120.213.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
2.53.134.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.120.213.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
176.13.236.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
202.83.120.30	Indonesia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
37.26.148.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.192.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.236.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.35.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.202.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.25.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.236.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.186	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
66.102.9.145	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
172.58.172.89	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
172.58.172.89	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.120.213.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.120.213.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.132.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.120.213.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.0.207.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.29.176.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.132.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.120.213.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
78.102.111.94	Czech Republic	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.13	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.109.1.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-28-2016-22:04:03 to 09-28-2016-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.187.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.144.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.81.63	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	2
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.192.147.82	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
79.178.38.169	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	2
5.102.241.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.90.120.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/71774.pdf‏	Block	2
31.154.81.63	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.57.61.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giuys	Block	1
46.19.86.26	Israel	147.237.76.42	refuah.idf.il	Malformed URL asp.net_sessionid=glkgvprzb4sm1455umm5bzfr	Block	1
2.53.45.217	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.192.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.82.227	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	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
180.76.15.19	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9004-he/refuah.aspx	Block	1
84.108.139.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8921-he/refuah.aspx	Block	1
217.69.133.226	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane/	Block	1
46.19.86.26	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method vc=0%7C48%2C0%7C49%2C0%7C50%2C0%7C1%2C7%7C52; in URL asp.net_sessionid=glkgvprzb4sm1455umm5bzfr	Block	1
2.53.178.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.219.14	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
184.70.213.162	Canada	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
85.65.190.124	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.76.28	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
141.226.161.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.120.126.25	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
46.19.86.26	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
93.172.132.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/71772.pdf‏	Block	1
2.53.6.186	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
50.192.147.82	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/aspx	Block	1
157.55.39.127	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
79.178.46.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/2/71772.pdf‏	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
204.79.180.44	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
46.19.86.26	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
2.53.38.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/71772.pdf	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1
157.55.39.234	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
79.183.25.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-28-2016-22:04:03 to 09-28-2016-23:04:03