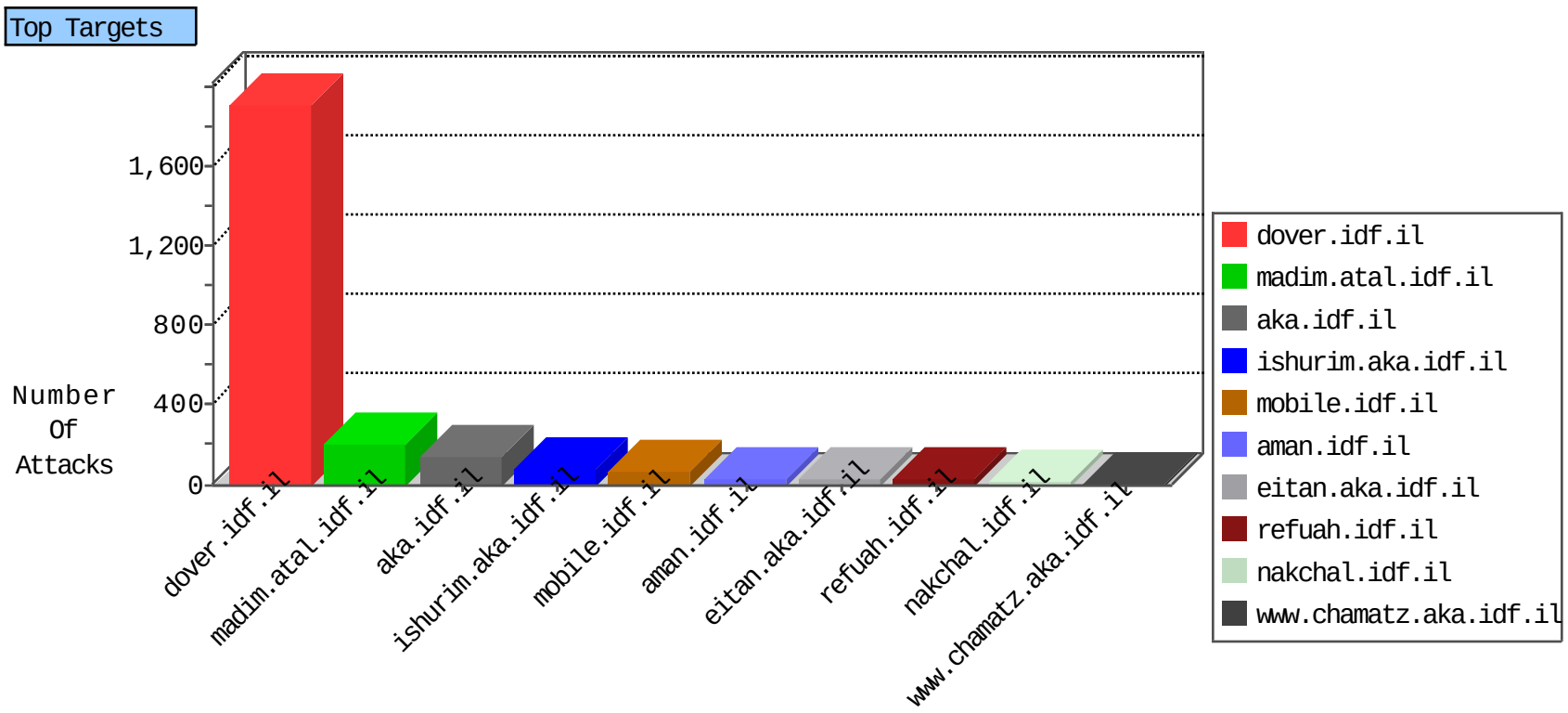
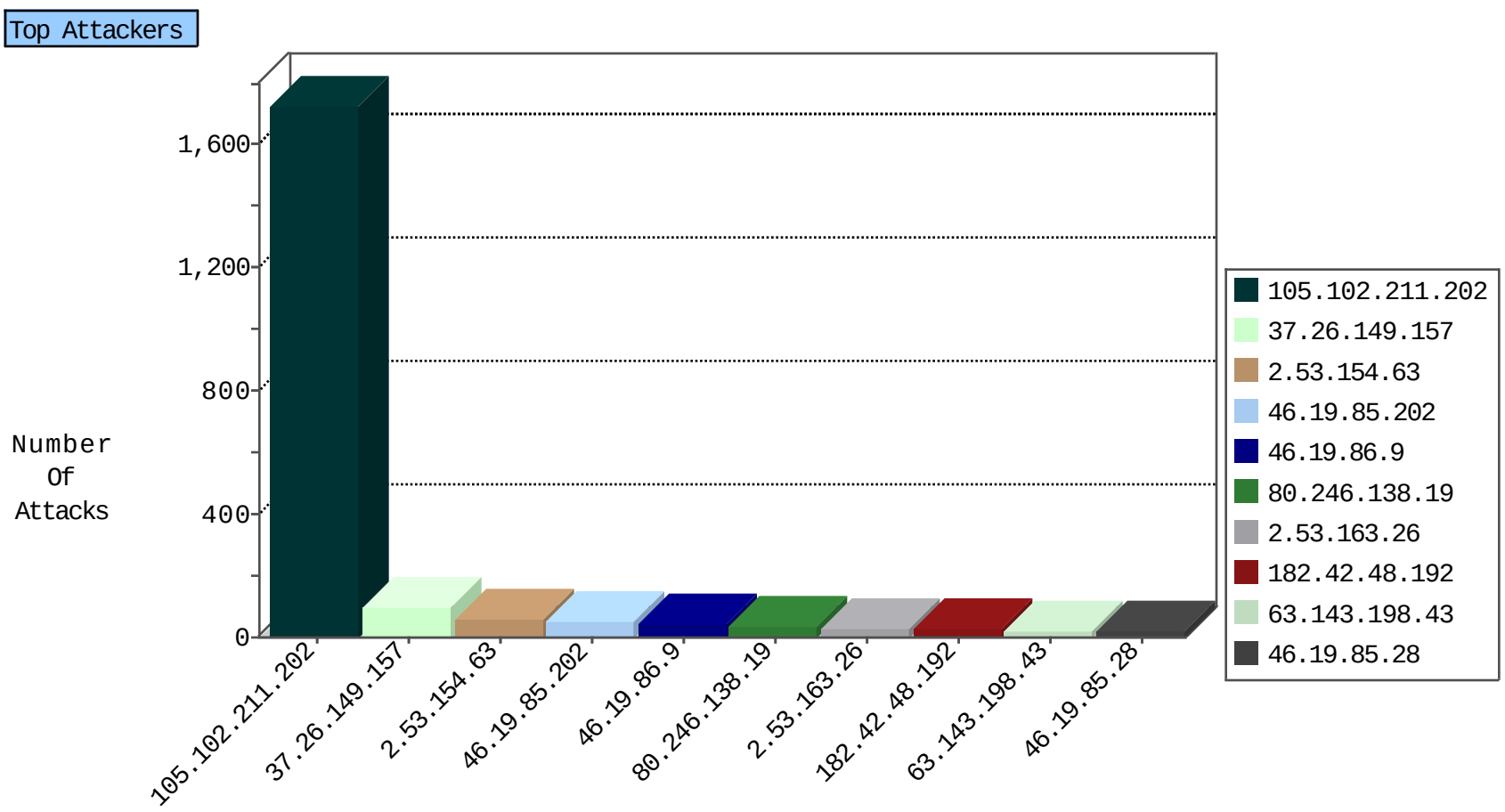
09-20-2016-08:04:05 to 09-20-2016-09:04:05

IDF Under Attack Daily Report





09-20-2016-08:04:05 to 09-20-2016-09:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.39.26	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
2.53.29.82	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
212.179.64.162	Israel	147.237.77.176	matpash.idf.il	Black List	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.22.150.78	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
128.208.4.197	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
195.62.53.168	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.14	dover.idf.il(old)	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
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	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
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.110.125.52	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1

09-20-2016-08:04:05 to 09-20-2016-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.101	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
173.31.183.87	United States	147.237.72.167	ishurim.aka.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-20-2016-08:04:05 to 09-20-2016-09:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	2
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
31.168.115.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.154.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.190.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
74.63.246.42	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
69.162.69.222	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.57.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.149.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.229.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.102.211.202	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
74.63.237.154	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

09-20-2016-08:04:05 to 09-20-2016-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.102.211.202	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1721
80.246.138.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.53.163.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.154.63	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
2.53.154.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	14
62.0.235.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
63.143.198.43	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.53.154.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
213.71.171.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
63.143.198.43	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
62.90.144.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.150.61.66	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
203.81.85.2	Myanmar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.154.63	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.53.169.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.244.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	6
213.57.12.56	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.244.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	6
46.19.86.65	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.196	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.196	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.242	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.154.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.140.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.53.154.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.236	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.226.17.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.194.206.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.40	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.130.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.244.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.120.134.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.176.73.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
2.55.32.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.202.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-20-2016-08:04:05 to 09-20-2016-09:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
182.42.48.192	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 182.42.48.192	Block	17
182.42.48.192	China	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	6
213.8.115.172	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
37.26.149.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
185.120.124.39	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
80.246.139.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.231.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.28.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.208.38	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugshikulim.aspx	Block	2
213.8.115.172	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	2
5.29.203.40	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.178.47.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
2.53.0.49	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
185.120.124.39	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1152-he/chinuch.aspx	Block	1
31.210.187.83	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
80.246.136.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
93.172.148.107	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58604&docid=73552	Block	1
213.8.115.172	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 213.8.115.172	Block	1
182.42.48.192	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
46.19.86.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl37 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.53.56.16	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
195.62.53.168	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
176.12.130.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
182.42.48.192	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/index.asp	Block	1
82.81.105.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
62.0.98.170	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.186.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.165	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
79.176.79.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
212.235.103.203	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1

09-20-2016-08:04:05 to 09-20-2016-09:04:05